TAMPEREEN YLIOPISTO
Pro gradu -tutkielma

Suvi Pasanen

Kvasiryhmistä ja niiden sovelluksista

Informaatiotieteiden yksikkö
Matematiikka
Maaliskuu 2016

Tampereen yliopisto
Informaatiotieteiden yksikkö
PASANEN, SUVI: Kvasiryhmistä ja niiden sovelluksista
Pro gradu -tutkielma, 38 s.
Matematiikka
Maaliskuu 2016

Tiivistelmä

Tutkielman aiheena ovat kvasiryhmiksi kutsutut algebralliset struktuurit. Lisäksi tutkielmassa esitellään kvasiryhmien sovelluksina latinalaiset neliöt sekä eräs kvasiryhmiä käyttävä salausalgoritmi. Kvasiryhmät ovat sellaisia struktuureja $(Q, *)$, joissa silloin, kun joukon Q alkioille pätee, että $x * y = z$ ja että alkioista kaksi tiedetään, niin kolmas pystytään päättelemään yksikäsitteisesti. Tutkielman luvussa 2 esitellään kvasiryhmien teoriaa. Luvussa määritellään kvasiryhmille vasemman- ja oikeanpuoleiset jakolaskut, joiden avulla voidaan esittää kvasiryhmille uusi karakterisointi. Lisäksi esitetään lause, jota kutsutaan alikvasiryhmätestiksi, jonka avulla pystytään selvittämään, muodostaako joukon osajoukko myös kvasiryhmän niissä määritellyllä laskutoimituksella. Luvussa määritellään myös kvasiryhmille homomorfiat ja isomorfiat sekä erityisesti homotopiat ja isotopiat. Tutkielmassa osoitetaan, että kvasiryhmäisotopia on ekvivalenssirelaatio. Lisäksi isotopioista erikoistapauksena määritellään myös pääisotopia, jossa kolmas isotopian komponenteista on identiteettikuvaus. Luvun lopuksi esitellään luupit, jotka ovat sellaisia kvasiryhmiä, joilla on neutraalialkio. Latinalaisten neliöiden määritelmän lisäksi tutkielman luvussa 3 esitetään muutamia merkittäviä lauseita, jotka yhdistävät kvasiryhmiä ja latinalaisia neliöitä sekä lisäksi siinä esitetään kvasiryhmien kertotauluesitys. Luvun lopuksi osoitetaan, että on olemassa kvasiryhmiä, jotka eivät ole isomorfisia ryhmien kanssa, mistä syystä kvasiryhmien tarkastelu ryhmistä erillisinä algebrallisina struktuureina on mielekästä. Tutkielman lopuksi luvussa 4 luodaan lyhyt katsaus kryptografian teoriaan ja esitellään sekä arvioidaan symmetristä jonosalausalgoritmia, joka käyttää salauksessa apunaan kvasiryhmiä.

Asiasanat: kvasiryhmä, latinalainen neliö, kryptografia

Sisältö

1 Johdanto

Tässä tutkielmassa esitellään algebrallisia struktuureja, joita kutsutaan kvasiryhmiksi. Luvussa 2 käsitellään kvasiryhmien yleistä teoriaa. Aliluvussa 2.1 esitetään kvasiryhmän määritelmä ja tuodaan esille sen ja ryhmän määritelmän eroavaisuuksia. Aliluvussa 2.2 määritellään kvasiryhmille kaksi erilaista jakolaskua, joiden avulla kvasiryhmille voidaan esittää uusi määritelmä. Aliluvussa 2.3 tarkastellaan kvasiryhmien alikvasiryhmiä ja esitellään alikvasiryhmätestiksi kutsuttu lause, jonka avulla pystytään määrittämään muodostaako kvasiryhmän joukon osajoukko myös kvasiryhmän. Aliluvussa 2.4 määritellään homomorfiat ja isomorfiat kvasiryhmien yhteydessä. Aliluvussa 2.5 esitetään kvasiryhmien homotopian ja isotopian määritelmät sekä esitetään miten kvasiryhmistä saadaan muodostettua isotopian avulla uusia kvasiryhmiä. Aliluvussa 2.6 määritellään pääisotopia, joka on isotopian erikoistapaus. Luvun lopuksi aliluvussa 2.7 esitellään luuppien määritelmä ja osoitetaan isotooppisten ryhmien olevan myös isomorfisia. Luvussa 3 määritellään latinalaiset neliöt ja esitellään kvasiryhmien eräs esitystapa, jolla on yhteys latinalaisiin neliöihin. Aliluvussa 3.2 myös esitetään esimerkkitapaus luupista, joka ei ole liitännäinen ja esitetään perustelu, miksi kvasiryhmien tarkastelu ryhmistä erillisenä algebrallisena struktuurina on mielekästä. Lopuksi luvussa 4 luodaan lyhyt katsaus kryptografiaan, esitellään eräs kvasiryhmiä soveltava salausalgoritmi sekä viimeiseksi arvioidaan algoritmia kryptografialle merkittävien ominaisuuksien valossa.

Tutkielman lukijalta oletetaan ryhmäteorian alkeiden tiedot, sillä esimerkiksi ryhmän määritelmää ei tutkielmassa esitetä. Pääosin tutkielmassa kuitenkin pyritään määrittelemään ja esittämään tarkasti siinä tehdyt päätelmät ja käytetyt termit. Tutkielman esimerkit ovat kirjoittajan itsensä keksimiä ja niihin on pyritty valitsemaan mahdollisimman yksinkertaiset joukot ja laskutoimitukset, joiden avulla aihealuetta pyritään selventämään lukijalle.

Pääasiallisena lähdeteoksena tutkielmassa on käytetty J. D. Smithin kirjaa *Introduction to Abstract Algebra*. Kyseinen kirja on muotoiltu siten, että todistuksista on usein jätetty osa lukijan harjoitustehtäväksi. Tutkielman todistuksissa pyritään tuomaan ilmi selkeästi, mikäli osa todistuksesta on tutkielman kirjoittajan osoittamaa. Tutkielmassa on käytetty lähteenä lähinnä latinalaisten neliöiden yhteydessä ja aliluvussa 2.5 esitetyssä kvasiryhmien muodostamisen esimerkissä myös C. Kościelnyn artikkelia *Generating quasigroups for cryptographic applications*. Lisäksi tutkielman kryptografisessa osuudessa merkittävimmät lähteet ovat S. Markovskin, D. Gligoroskin ja S. Andovan konferenssiartikkeli *Using quasigroups for one-one secure encoding* ja E. Ochodkovan and V. Snášelin konferenssiartikkeli *Using quasigroups for secure encoding of file system*. Tutkielmassa on pyritty mahdollisimman tarkkaan lähdeviittaustapaan ja muut tutkielmassa käytetyt lähteet ilmenevät niiden esiintymiskohdissa.

2 Kvasiryhmien ominaisuuksia

2.1 Kvasiryhmän määritelmä

Ryhmäteoriassa ryhmän $(Q, \cdot)$ laskutoimituksella on kaksi tärkeää ominaisuutta: liitännäisyys ja se, että mikäli x, y ja z ovat joukon Q alkioita, joille $x \cdot y = z$ ja niistä kaksi tiedetään, pystytään kolmas päättelemään yksikäsitteisesti. On olemassa myös joukkoja, joiden laskutoimitus täyttää vain toisen näistä ehdoista. Joukkoja, jotka täyttävät vain liitännäisyyden ehdon, kutsutaan puoliryhmiksi. [7, s. 287] Tässä tutkielmassa esitellään jälkimmäisen ehdon toteuttavat joukot, joita kutsutaan kvasiryhmiksi.

Määritelmä 2.1.1 (vrt. [7, s. 287])**.** Olkoon joukko Q suljettu sen alkioiden laskutoimituksen $\cdot$ suhteen. Oletetaan, että kun joukon Q alkioille x, y ja z pätee, että

$$x \cdot y = z$$

ja että näistä alkioista kaksi tiedetään, niin kolmas alkio pystytään päättelemään yksikäsitteisesti. Silloin struktuuria $(Q, \cdot)$ kutsutaan *kvasiryhmäksi*.

Tyhjä joukko toteuttaa kvasiryhmän määritelmän, sillä siinä ei ole alkioita, joille määritelmän väite voitaisiin osoittaa epätodeksi. Osassa lähteistä kuitenkin määritellään struktuurin $(Q, \cdot)$ joukko Q epätyhjäksi. [5, s. 2] Myös tässä tutkielmassa oletetaan, että joukko Q ei ole tyhjä joukko. Lisäksi on huomioitava, että tässä tutkielmassa struktuurin $(Q, \cdot)$ laskutoimitusta $\cdot$ kutsutaan *kertolaskuksi*, mutta kyseessä voi olla mikä tahansa joukossa Q määritelty kahden alkion laskutoimitus.

Esimerkki 2.1.1. Tarkastellaan reaalilukujen joukkoa $\mathbb{R}$ varustettuna tavallisella reaalilukujen vähennyslaskulla, eli struktuuria $(\mathbb{R}, -)$. Oletetaan, että reaaliluvuille x, y ja z pätee $x - y = z$. Jos alkiot x ja y tiedetään, niin reaalilukujen vähennyslaskulla voidaan määrittää alkion z yksikäsitteisesti. Jos tiedetään alkiot x ja z, niin y voidaan määrittää yksikäsitteisesti yhtälöstä $y = x - z$. Mikäli tiedetään alkiot y ja z, voidaan x määrittää yksikäsitteisesti yhtälöstä $x = y + z$. Täten $(\mathbb{R}, -)$ on kvasiryhmä.

Huomioitavaa on, että struktuurissa $(\mathbb{R}, -)$ pätee esimerkiksi

$$(1 - 1) - 1 = -1 \neq 1 = 1 - (1 - 1),$$

joten $(\mathbb{R}, -)$ ei ole liitännäinen. Täten $(\mathbb{R}, -)$ ei ole ryhmä. Näin ollen kaikki kvasiryhmät eivät ole ryhmiä.

Lause 2.1.1. *Jokainen ryhmä on kvasiryhmä.*

Todistus. (Vrt. [7, s. 86]). Olkoon struktuuri $(Q, \cdot)$ ryhmä. Oletetaan myös, että $x \cdot y = z$, joillain x, y, $z \in Q$. Nyt tulee osoittaa, että mikäli kaksi alkioista x, y ja z tiedetään, niin kolmas pystytään määrittämään yksikäsitteisesti. Jos x ja y tiedetään, niin z voidaan määrittää yksikäsitteisesti ryhmän Q kertolaskun mukaisesti. Jos x ja z tiedetään, niin y voidaan selvittää ratkaisemalla $y = x^{-1} \cdot z$, missä x^{-1} on alkion x käänteisalkio joukossa Q. Tämä pätee, sillä

$$x \cdot y = x \cdot (x^{-1} \cdot z) = (x \cdot x^{-1}) \cdot z = e \cdot z = z,$$

missä e on ryhmän $(Q, \cdot)$ neutraalialkio, ja koska lisäksi tiedetään, että ryhmille pätee, että kun x, y_1 ja y_2 ovat ryhmän alkioita, niin

$$x \cdot y_1 = x \cdot y_2 \implies y_1 = y_2.$$

Jos y ja z tiedetään, voidaan x ratkaista yksikäsitteisesti yhtälöstä $x = z \cdot y^{-1}$. Tämä pätee, sillä

$$x \cdot y = (z \cdot y^{-1}) \cdot y = z \cdot (y \cdot y^{-1}) = z \cdot e = z,$$

missä e on ryhmän $(Q, \cdot)$ neutraalialkio ja koska lisäksi tiedetään, että ryhmille pätee, että kun x_1, x_2 ja y ovat ryhmän alkioita, niin

$$x_1 \cdot y = x_2 \cdot y \implies x_1 = x_2.$$

□

2.2 Kvasiryhmän jakolaskut

Kvasiryhmät on määritelty siten, että niissä voidaan suorittaa myös laskutoimituksen käänteisoperaatio, jota tässä tutkielmassa kutsutaan jakolaskuksi. Itse asiassa kvasiryhmissä voidaan määritellä kaksi erilaista jakolaskua.

Määritelmä 2.2.1 (vrt. [7, s. 293])**.** Olkoon $(Q, \cdot)$ kvasiryhmä ja olkoot x ja y joukon Q alkioita. Tällöin joukon Q alkio $x\backslash y$ määritellään yhtälön

$$x \cdot z = y$$

yksikäsitteisenä ratkaisuna z. Toisin sanoen,

$$x \cdot (x\backslash y) = y.$$

Joukon Q laskutoimitusta $\backslash$ kutsutaan *kvasiryhmän* $(Q, \cdot)$ *vasemmanpuoleiseksi jakolaskuksi.*

Määritelmä 2.2.2 (vrt. [7, s. 293])**.** Olkoon $(Q, \cdot)$ kvasiryhmä ja olkoot x ja y joukon Q alkioita. Tällöin joukon Q alkio x/y määritellään yhtälön

$$z \cdot y = x$$

yksikäsitteisenä ratkaisuna z. Toisin sanoen,

$$(x/y) \cdot y = x.$$

Joukon Q laskutoimitusta / kutsutaan *kvasiryhmän* $(Q, \cdot)$ *oikeanpuoleiseksi jakolaskuksi.*

Esimerkki 2.2.1. Tarkastellaan reaalilukujen joukkoa $\mathbb{R}$ vähennyslaskulla varustettuna. Esimerkissä 2.1.1 osoitettiin, että $(\mathbb{R}, -)$ on kvasiryhmä. Kvasiryhmässä $(\mathbb{R}, -)$ alkio $1\backslash 2$ saadaan ratkaisemalla yhtälö

$$\begin{aligned} 1 - (1\backslash 2) &= 2, \\ (1\backslash 2) &= 1 - 2, \\ (1\backslash 2) &= -1. \end{aligned}$$

Toisin sanoen kvasiryhmän $(\mathbb{R}, -)$ vasemmanpuoleisessa jakolaskussa osoittajasta vähennetään nimittäjä. Toisaalta kvasiryhmän $(\mathbb{R}, -)$ alkio $1/2$ saadaan ratkaisemalla yhtälö

$$\begin{aligned} (1/2) - 2 &= 1, \\ (1/2) &= 1 + 2, \\ (1/2) &= 3. \end{aligned}$$

Kvasiryhmän $(\mathbb{R}, -)$ oikeanpuoleinen jakolasku on täten osoittajan ja nimittäjän summa.

Apulause 2.2.1. *Olkoon $(Q, \cdot)$ kvasiryhmä ja olkoot x ja y joukon Q alkioita. Tällöin seuraavat ominaisuudet ovat voimassa:*

1. $x\backslash(x \cdot y) = y$,
2. $y/(x\backslash y) = x$,
3. $(y \cdot x)/x = y$,
4. $(y/x)\backslash y = x$.

Todistus. (Vrt. [7, s. 295]). Olkoon $z = x \cdot y$. Tarkastellaan ensin väitettä 1. Koska $(Q, \cdot)$ on kvasiryhmä, niin alkio y on yhtälön $x \cdot s = z$ yksikäsitteinen ratkaisu s. Toisaalta vasemmanpuoleisen jakolaskun määritelmän 2.2.1 nojalla tiedetään, että $x \cdot (x\backslash z) = z$, joten on oltava $y = x\backslash z$. Tällöin

$$\begin{aligned} x\backslash(x \cdot y) &= x\backslash(x \cdot (x\backslash z)) \\ &= x\backslash z \\ &= y, \end{aligned}$$

eli väite 1 pätee.

Tarkastellaan seuraavaksi väitettä 2. Oikeanpuoleisen jakolaskun määritelmän 2.2.2 mukaan $(z/y) \cdot y = z$. Koska $(Q, \cdot)$ on kvasiryhmä, niin alkio x on yhtälön $t \cdot y = z$ yksikäsitteinen ratkaisu t. Täten on oltava $z/y = x$. Nyt

$$\begin{aligned} z/(x\backslash z) &= z/y \\ &= x. \end{aligned}$$

Nähdään, että selvästi väite 2 pätee, kun edelliseen yhtälöön alkion z paikalle sijoitetaan alkio y.

Lähteessä [7] väitteiden 3 ja 4 todistus on jätetty harjoitustehtäväksi. Osoitetaan ne todeksi tässä tutkielmassa. Tarkastellaan ensiksi väitettä 3. Olkoon z' se yksikäsitteinen joukon Q alkio, jolle pätee $y \cdot x = z'$. Oikeanpuoleisen jakolaskun määritelmän 2.2.2 nojalla $(z'/x) \cdot x = z' = y \cdot x$, eli $z'/x = y$. Saadaan

$$\begin{aligned} (y \cdot x)/x &= z'/x \\ &= y, \end{aligned}$$

eli väite 3 pätee.

Tarkastellaan vielä väitettä 4. Vasemmanpuoleisen jakolaskun määritelmän 2.2.1 nojalla $y \cdot (y\backslash z') = z' = y \cdot x$, eli $y\backslash z' = x$. Nyt väitteen 3 nojalla pätee

$$\begin{aligned} (z'/x)\backslash z' &= ((y \cdot x)/x)\backslash z' \\ &= y\backslash z' \\ &= x. \end{aligned}$$

Nähdään, että selvästi väite 4 pätee, kun edelliseen yhtälöön alkion z' paikalle sijoitetaan alkio y. □

Nyt voidaan jakolaskun avulla esittää uusi määritelmä kvasiryhmille.

Lause 2.2.2. *Joukko Q muodostaa kvasiryhmän $(Q, \cdot)$ jos ja vain jos siinä määritellyille vasemmanpuoleiselle ja oikeanpuoleiselle jakolaskulle pätee:*

1. $x \cdot (x\backslash y) = y$,
2. $(x/y) \cdot y = x$,
3. $x\backslash(x \cdot y) = y$,
4. $(y \cdot x)/x = y$,

kaikilla $x, y \in Q$.

Todistus. (Vrt. [7, s. 295]). Oletetaan ensin, että $(Q, \cdot)$ on kvasiryhmä. Tällöin väite 1 seuraa suoraan vasemmanpuoleisen jakolaskun määritelmästä 2.2.1 ja väite 2 seuraa suoraan oikeanpuoleisen jakolaskun määritelmästä 2.2.2. Lisäksi apulauseen 2.2.1 nojalla väitteet 3 ja 4 pätevät, sillä väite 3 on apulauseen ominaisuus 1 ja väite 4 on apulauseen ominaisuus 3.

Oletetaan sitten, että joukossa Q on määritelty operaatiot $\cdot$, $\backslash$ ja $/$ siten, että niille pätee väitteet 1 - 4. Tarkastellaan yhtälöä $x \cdot y = z$, kun x, y ja z kuuluvat joukkoon Q. Huomataan ensin, että jos x ja y tiedetään, niin yksikäsitteinen ratkaisu z saadaan joukon Q kertolaskun määritelmän mukaisesti. Osoitetaan sitten, että yhtälölle $x \cdot y = z$ löytyy yksikäsitteinen ratkaisu joukosta Q, kun tiedetään alkiot y ja z. Tällöin väitteen 2 nojalla $(z/y) \cdot y = z$, joten $x = z/y$ on yksi ratkaisu yhtälölle $x \cdot y = z$. Oletetaan sitten joukon Q alkioiden s ja t olevan ratkaisuja yhtälölle $x \cdot y = z$, kun y ja z tiedetään. Väitteen 4 perusteella saadaan

$$s = (s \cdot y)/y = z/y = (t \cdot y)/y = t.$$

Täten saatu ratkaisu $x = z/y$ on yksikäsitteinen. Osoitetaan vielä lopuksi lähteessä [7] harjoitustehtäväksi jätetty tilanne, missä yhtälölle $x \cdot y = z$ löytyy ratkaisu joukosta Q, kun tiedetään alkiot x ja z. Tällöin väitteen 1 perusteella $x \cdot (x\backslash z) = z$ eli $y = x\backslash z$ on yksi yhtälön $x \cdot y = z$ ratkaisu. Oletetaan alkioiden $s', t' \in Q$ olevan ratkaisuja yhtälölle $x \cdot y = z$, kun x ja z tiedetään. Nyt väitteen 3 nojalla

$$s' = x\backslash(x \cdot s') = x\backslash z = x\backslash(x \cdot t') = t'.$$

Siis ratkaisu $y = x\backslash z$ on yksikäsitteinen. Täten on osoitettu, että $(Q, \cdot)$ on kvasiryhmä. □

Lause 2.2.3. *Olkoon $(Q, \cdot)$ kvasiryhmä, jossa on määritelty vasemmanpuoleinen jakolasku $\backslash$ ja oikeanpuoleinen jakolasku $/$. Tällöin struktuurit $(Q, \backslash)$ ja $(Q, /)$ ovat myös kvasiryhmiä.*

Todistus. (Vrt. [7, s. 296]). Tarkastellaan yhtälöä $x\backslash y = z$, jossa $x, y, z \in Q$. Jos alkiot x ja y tiedetään, niin z voidaan ratkaista yhtälöstä vasemmanpuoleisen jakolaskun määritelmän 2.2.1 perusteella yksikäsitteisesti. Oletetaan sitten, että tiedetään alkiot y ja z. Apulauseen 2.2.1 ominaisuuden 4 nojalla tiedetään, että yhtälöllä on ratkaisu $x = y/z$. Jos olisi olemassa sellainen $s \in Q$, että $s\backslash y = z$ ja $x\backslash y = z$, niin apulauseen 2.2.1 väitteen 2 nojalla

$$x = y/z = y/(s\backslash y) = s.$$

Täten saatu ratkaisu $x = y/z$ on yksikäsitteinen.

Todistuksen seuraavat osiot on jätetty lähteessä [7] harjoitustehtäviksi. Osoitetaan ne tässä tutkielmassa todeksi. Tarkastellaan vielä tapausta, jossa yhtälöstä $x\backslash y = z$ tiedetään alkiot x ja z. Apulauseen 2.2.1 ominaisuuden 1 nojalla yhtälöllä on ratkaisu $y = x \cdot z$. Oletetaan, että on olemassa sellainen $s' \in Q$, jolle $x\backslash s' = z$. Nyt koska $(Q, \cdot)$ on kvasiryhmä, niin vasemmanpuoleisen jakolaskun määritelmän 2.2.1 nojalla pätee

$$y = x \cdot (x\backslash y) = x \cdot z = x \cdot (x\backslash s') = s'.$$

Täten on osoitettu, että $(Q, \backslash)$ on kvasiryhmä.

Tarkastellaan sitten yhtälöä $x/y = z$, jossa x, y, $z \in Q$. Jos alkiot x ja y tiedetään, niin z voidaan ratkaista yhtälöstä oikeanpuoleisen jakolaskun määritelmän 2.2.2 perusteella yksikäsitteisesti. Oletetaan, että tiedetään alkiot y ja z. Lauseen 2.2.2 ominaisuuden 4 nojalla yhtälöllä on ratkaisu $x = z \cdot y$. Jos olisi olemassa $t \in Q$ siten, että $t/y = z$ ja $x/y = z$, niin lauseen 2.2.2 ominaisuudesta 2 seuraa, että

$$x = z \cdot y = (t/y) \cdot y = t.$$

Täten saatu ratkaisu $x = z \cdot y$ on yksikäsitteinen. Oletetaan vielä, että tiedetään alkiot x ja z. Tällöin apulauseen 2.2.1 ominaisuuden 2 nojalla yhtälöllä on ratkaisu $y = z\backslash x$. Oletetaan, että on olemassa sellainen $t' \in Q$, että $x/t' = z$. Tällöin apulauseen 2.2.1 ominaisuuden 4 nojalla pätee

$$y = z\backslash x = (x/t')\backslash x = t'.$$

Täten saatu ratkaisu $y = z\backslash x$ on yksikäsitteinen ja on osoitettu, että $(Q, /)$ on kvasiryhmä. □

2.3 Alikvasiryhmät

Tässä aliluvussa esitellään alikvasiryhmien käsite. Lisäksi esitellään lause, jonka avulla voidaan selvittää, onko joukon osajoukko myös kvasiryhmä.

Määritelmä 2.3.1 (vrt. [7, s. 297])**.** Olkoon $(Q, \cdot)$ kvasiryhmä. Jos joukon Q osajoukko S muodostaa kvasiryhmän $(S, \cdot)$, sitä kutsutaan kvasiryhmän $(Q, \cdot)$ *alikvasiryhmäksi.*

Lause 2.3.1 (Alikvasiryhmätesti)**.** *Olkoon $(Q, \cdot)$ kvasiryhmä ja olkoon S joukon Q osajoukko. Tällöin $(S, \cdot)$ on kvasiryhmän $(Q, \cdot)$ alikvasiryhmä, jos ja vain jos kaikille x, $y \in S$ pätee, että $x \cdot y$, $x\backslash y$ ja $x/y \in S$.*

Todistus. (Vrt. [7, s. 298]). Jos S on suljettu kertolaskun sekä vasemman- ja oikeanpuoleisen jakolaskun suhteen, niin lauseen 2.2.2 nojalla voidaan todeta, että $(S, \cdot)$ on kvasiryhmä. Alikvasiryhmän määritelmän 2.3.1 nojalla $(S, \cdot)$ on siis kvasiryhmän $(Q, \cdot)$ alikvasiryhmä.

Oletetaan sitten, että $(S, \cdot)$ on kvasiryhmän $(Q, \cdot)$ alikvasiryhmä. Tällöin $(S, \cdot)$ on alikvasiryhmän määritelmän 2.3.1 nojalla myös kvasiryhmä. Oletetaan, että x ja y ovat joukon S alkioita. Tällöin kvasiryhmän määritelmästä 2.1.1 seuraa että $x \cdot y \in S$. Täten $(S, \cdot)$ on suljettu kertolaskun suhteen. Tiedetään myös, että yhtälön $x \cdot z = y$ yksikäsitteisen ratkaisun $z = z_S \in S$ tulee olla sama kuin yksikäsitteisen ratkaisun $z = z_Q \in Q$, sillä joukoissa S ja Q on määritelty sama laskutoimitus. Tämä ratkaisu voidaan vasemmanpuoleisen jakolaskun määritelmän 2.2.1 mukaan kirjoittaa $z = x\backslash y$. Näin ollen $(S, \cdot)$ on suljettu vasemmanpuoleisen jakolaskun suhteen. Toisaalta yhtälön $z' \cdot y = x$ yksikäsitteisen ratkaisun $z' = z'_S \in S$ tulee olla sama kuin yksikäsitteisen ratkaisun $z' = z'_Q \in Q$. Tämä ratkaisu voidaan oikeanpuoleisen jakolaskun määritelmän 2.2.2 mukaan kirjoittaa $z' = x/y$. Täten kvasiryhmä $(S, \cdot)$ on suljettu myös oikeanpuoleisen jakolaskun suhteen. □

Esimerkki 2.3.1. Onko kokonaislukujen joukko $\mathbb{Z}$ vähennyslaskulla varustettuna kvasiryhmä? Tiedetään, että $\mathbb{Z}$ on reaalilukujen joukon $\mathbb{R}$ osajoukko. Esimerkissä 2.1.1 osoitettiin reaalilukujen joukon $\mathbb{R}$ varustettuna vähennyslaskulla olevan kvasiryhmä. Esimerkissä 2.2.1 osoitettiin, että kvasiryhmässä $(\mathbb{R}, -)$ vasemmanpuoleisen jakolaskun $x\backslash y$ tulos saadaan vähentämällä nimittäjästä osoittaja. Tunnetusti kaikille x ja $y \in \mathbb{Z}$ pätee, että $x - y \in \mathbb{Z}$, joten $x\backslash y = x - y \in \mathbb{Z}$. Esimerkissä 2.2.1 osoitettiin myös, että oikeanpuoleisen jakolaskun x/y tulos saadaan laskemalla osoittaja ja nimittäjä yhteen. Koska kaikille x ja $y \in \mathbb{Z}$ pätee, että $x + y \in \mathbb{Z}$, niin myös $x/y \in \mathbb{Z}$. Täten lauseen 2.3.1 nojalla $(\mathbb{Z}, -)$ on kvasiryhmä.

Esimerkki 2.3.2. Onko luonnollisten lukujen joukko $\mathbb{N}$ vähennyslaskulla varustettuna kvasiryhmä? Tiedetään, että $\mathbb{N}$ on reaalilukujen joukon $\mathbb{R}$ osajoukko. Esimerkissä 2.1.1 osoitettiin reaalilukujen joukon $\mathbb{R}$ varustettuna vähennyslaskulla olevan kvasiryhmä. Tarkastellaan lukuja 1 ja $2 \in \mathbb{N}$. Nyt esimerkin 2.2.1 nojalla vasemmanpuoleinen jakolasku olisi $1\backslash 2 = 1 - 2 = -1 \notin \mathbb{N}$. Täten $(\mathbb{N}, -)$ ei ole kvasiryhmä.

2.4 Homomorfiat ja isomorfiat

Määritelmä 2.4.1 (vrt. [7, s. 298])**.** Olkoot $(Q_1, \cdot)$ ja $(Q_2, *)$ kvasiryhmiä. Tällöin kuvaus $f : Q_1 \to Q_2$ on *kvasiryhmähomomorfismi*, jos

$$f(x) * f(y) = f(x \cdot y) \qquad \forall x, y \in Q_1.$$

Määritelmä 2.4.2 (vrt. [7, s. 298])**.** Olkoot $(Q_1, \cdot)$ ja $(Q_2, *)$ kvasiryhmiä ja olkoon $f : (Q_1, \cdot) \to (Q_2, *)$ kvasiryhmähomomorfismi. Jos f on bijektio, sitä kutsutaan *kvasiryhmäisomorfismiksi*. Kvasiryhmät Q_1 ja Q_2 ovat *isomorfiset*, jos niiden välillä on isomorfismi.

Esimerkki 2.4.1. Tarkastellaan reaalilukujen joukkoa $\mathbb{R}$ ja positiivisten reaalilukujen joukkoa $\mathbb{R}^+$. Määritellään kahden reaaliluvun x ja y *aritmeettisen keskiarvon* $*$ olevan

$$x * y = \frac{x + y}{2}.$$

Määritellään lisäksi kahden positiivisen reaaliluvun x' ja y' *geometrisen keskiarvon* $\circ$ olevan

$$x' \circ y' = \sqrt{x' \cdot y'}.$$

Osoitetaan, että struktuurit $(\mathbb{R}, *)$ ja $(\mathbb{R}^+, \circ)$ ovat kvasiryhmiä ja että niiden välillä on kvasiryhmäisomorfia. Oletetaan, että $x * y = z$ pätee joillain reaaliluvuilla x, y ja z. Jos tiedetään x ja y, niin selvästi niiden aritmeettinen keskiarvo $z = \frac{x+y}{2}$ on yksikäsitteisesti määritelty. Jos taas tiedetään y ja z, niin x voidaan määrittää yksikäsitteisesti $x = 2z - y$. Lisäksi mikäli tiedetään x ja z,

niin y voidaan määrittää yhtälöstä $y = 2z - x$ yksikäsitteisesti. Täten $(\mathbb{R}, *)$ on kvasiryhmä.

Oletetaan sitten, että $x \circ y = z$ pätee joillain positiivisilla reaaliluvuilla x, y ja z. Kun tiedetään x ja y, niiden geometrinen keskiarvo $z = \sqrt{x \cdot y}$ on selvästi yksikäsitteisesti määritelty. Jos y ja z tiedetään, niin x on yksikäsitteisesti määritettynä $x = \frac{z^2}{y}$. Jos taas x ja z tiedetään, niin y voidaan määrittää yksikäsitteisesti $y = \frac{z^2}{x}$. Siis myös $(\mathbb{R}^+, \circ)$ on kvasiryhmä.

Olkoon funktio $f : (\mathbb{R}, *) \to (\mathbb{R}^+, \circ)$ määritelty siten, että $f : x \mapsto e^x$. Tiedetään, että eksponenttifunktiona f on bijektio. Riittää siis osoittaa, että f on kvasiryhmähomomorfismi. Olkoot a, $b \in \mathbb{R}$. Nyt

$$\begin{aligned} f(a) \circ f(b) &= e^a \circ e^b \\ &= \sqrt{e^a \cdot e^b} \\ &= \sqrt{e^{(a+b)}} \\ &= (e^{(a+b)})^{\frac{1}{2}} \\ &= e^{(a+b)(\frac{1}{2})} \\ &= e^{\frac{a+b}{2}} \\ &= f(a * b). \end{aligned}$$

On siis osoitettu, että kvasiryhmät $(\mathbb{R}, *)$ ja $(\mathbb{R}^+, \circ)$ ovat isomorfiset.

Lause 2.4.1. *Olkoot $(Q_1, \cdot)$ ja $(Q_2, *)$ kvasiryhmiä. Olkoon $f : Q_1 \to Q_2$ kvasiryhmäisomorfismi. Tällöin $(Q_1, \cdot)$ on liitännäinen, jos ja vain jos $(Q_2, *)$ on liitännäinen.*

Todistus. (Ks. [9, s. 39]). Oletetaan, että $(Q_1, \cdot)$ on liitännäinen. Nyt koska f on isomorfismina bijektio, niin se on myös surjektio. Täten kaikilla x, y ja $z \in Q_2$ pätee, että on olemassa sellaiset alkiot x', y' ja $z' \in Q_1$, joille $f(x') = x$, $f(y') = y$ ja $f(z') = z$. Tällöin pätee

$$\begin{aligned} (x * y) * z &= (f(x') * f(y')) * f(z') \\ &= f(x' \cdot y') * f(z') \\ &= f((x' \cdot y') \cdot z') \\ &= f(x' \cdot (y' \cdot z')) \\ &= f(x') * f(y' \cdot z') \\ &= f(x') * (f(y') * f(z')) \\ &= x * (y * z). \end{aligned}$$

Nähdään, että nyt myös $(Q_2, *)$ on liitännäinen.

Oletetaan sitten, että $(Q_2, *)$ on liitännäinen. Koska f on isomorfismi, niin

myös $f^{-1} : Q_2 \to Q_1$ on isomorfismi. Nyt pätee

$$\begin{aligned}(x' \cdot y') \cdot z' &= (f^{-1}(x) \cdot f^{-1}(y)) \cdot f^{-1}(z) \\ &= f^{-1}(x * y) \cdot f^{-1}(z) \\ &= f^{-1}((x * y) * z) \\ &= f^{-1}(x * (y * z)) \\ &= f^{-1}(x) \cdot f^{-1}(y * z) \\ &= f^{-1}(x) \cdot (f^{-1}(y) \cdot f^{-1}(z)) \\ &= x' \cdot (y' \cdot z'),\end{aligned}$$

eli myös $(Q_1, \cdot)$ on liitännäinen. Täten väite pätee. □

Lause 2.4.2. *Olkoot $(Q_1, \cdot)$ ja $(Q_2, \cdot)$ kvasiryhmiä, joille on määritelty vasemmanpuoleinen jakolasku $\backslash$ ja oikeanpuoleinen jakolasku $/$. Olkoon $f : (Q_1, \cdot) \to (Q_2, \cdot)$ kvasiryhmähomomorfismi. Tällöin kaikille x, $y \in Q_1$ pätee*

$$f(x)\backslash f(y) = f(x\backslash y) \qquad ja \qquad f(x)/f(y) = f(x/y).$$

Todistus. (Vrt. [7, s. 299]). Vasemmanpuoleisen jakolaskun määritelmän 2.2.1 perusteella kvasiryhmässä $(Q_1, \cdot)$ pätee $x \cdot (x\backslash y) = y$. Koska f on kvasiryhmähomomorfismi, niin

$$f(x) \cdot f(x\backslash y) = f(x \cdot (x\backslash y)) = f(y)$$

pätee joukossa Q_2. Toisaalta yhtälön $f(x) \cdot z = f(y)$ yksikäsitteinen ratkaisu kvasiryhmässä $(Q_2, \cdot)$ on vasemmanpuoleisen jakolaskun määritelmän 2.2.1 mukaan $z = f(x)\backslash f(y)$. Siis oltava $f(x)\backslash f(y) = f(x\backslash y)$.

Oikeanpuoleisen jakolaskun määritelmän 2.2.2 nojalla kvasiryhmässä $(Q_1, \cdot)$ pätee, että $(x/y) \cdot y = x$. Koska f on kvasiryhmähomomorfismi, niin joukossa Q_2 pätee

$$f(x/y) \cdot f(y) = f((x/y) \cdot y) = f(x).$$

Toisaalta yhtälön $z \cdot f(y) = f(x)$ yksikäsitteinen ratkaisu kvasiryhmässä $(Q_2, \cdot)$ on oikeanpuoleisen jakolaskun määritelmän 2.2.2 mukaan $z = f(x)/f(y)$. Siis pätee $f(x)/f(y) = f(x/y)$. □

Lause 2.4.3. *Olkoot $(Q_1, \cdot)$ ja $(Q_2, \cdot)$ kvasiryhmiä. Tällöin niiden karteesinen tulo $Q_1 \times Q_2$ varustettuna alkioiden kertolaskulla*

$$(x_1, x_2) \cdot (y_1, y_2) = (x_1 \cdot y_1, x_2 \cdot y_2)$$

muodostaa kvasiryhmän $(Q_1 \times Q_2, \cdot)$. Tässä kvasiryhmässä on vasemmanpuoleinen jakolasku

$$(x_1, x_2)\backslash(y_1, y_2) = (x_1\backslash y_1, x_2\backslash y_2)$$

ja oikeanpuoleinen jakolasku

$$(x_1, x_2)/(y_1, y_2) = (x_1/y_1, x_2/y_2),$$

kun ne toteutetaan alkioittain samoin, kuin kvasiryhmissä $(Q_1, \cdot)$ ja $(Q_2, \cdot)$.

Todistus. (Vrt. [7, s. 299]). Olkoot (x_1, x_2) ja (y_1, y_2) tunnettuja alkioita joukossa $Q_1 \times Q_2$. Tällöin niiden kertolaskun määritelmän mukaan pätee $(x_1, x_2) \cdot (y_1, y_2) = (x_1 \cdot y_1, x_2 \cdot y_2)$. Karteesisen tulon määritelmän perusteella tiedetään, että x_1,$y_1 \in Q_1$ ja x_2, $y_2 \in Q_2$. Koska $(Q_1, \cdot)$ ja $(Q_2, \cdot)$ ovat kvasiryhmiä, ne ovat kertolaskun suhteen suljettuja ja niissä kertolaskun tulos on yksikäsitteinen. Täten myös alkioiden kertolaskun tulos $(x_1 \cdot y_1, x_2 \cdot y_2)$ on yksikäsitteinen ja kuuluu joukkoon $Q_1 \times Q_2$.

Olkoot sitten (y_1, y_2) ja (z_1, z_2) tunnettuja alkioita joukossa $Q_1 \times Q_2$. Jos pätee, että

$$(x_1, x_2) \cdot (y_1, y_2) = (x_1 \cdot y_1, x_2 \cdot y_2) = (z_1, z_2),$$

jollakin $(x_1, x_2) \in Q_1 \times Q_2$, niin yhtälölle on olemassa ratkaisu

$$(x_1, x_2) = (z_1/y_1, z_2/y_2),$$

missä / on kvasiryhmien $(Q_1, \cdot)$ ja $(Q_2, \cdot)$ oikeanpuoleinen jakolasku. Lähteessä [7] todistuksen seuraavat osiot on jätetty harjoitustehtäväksi. Osoitetaan ne tässä tutkielmassa todeksi. Selvennetään kuitenkin vielä ensin saatua edellisestä kohdasta ratkaisua $(x_1, x_2) = (z_1/y_1, z_2/y_2)$, joka pätee, sillä

$$\begin{aligned}(z_1/y_1, z_2/y_2) \cdot (y_1, y_2) &= ((z_1/y_1) \cdot y_1, (z_2/y_2) \cdot y_2) \\ &= (z_1, z_2) \qquad \text{(lause 2.2.2, ominaisuus 2)}\end{aligned}$$

Tiedetään, että $z_1, y_1 \in Q_1$ ja $z_2, y_2 \in Q_2$. Oikeanpuoleisen jakolaskun määritelmän 2.2.2 mukaan sen tulos on yksikäsitteinen ja kuuluu kvasiryhmään. Täten saatu ratkaisu (x_1, x_2) on myös yksikäsitteinen ja $(x_1, x_2) \in Q_1 \times Q_2$.

Oletetaan vielä, että tunnetaan joukon $Q_1 \times Q_2$ alkiot (x_1, x_2) ja (z_1, z_2), joille pätee

$$(x_1, x_2) \cdot (y_1, y_2) = (x_1 \cdot y_1, x_2 \cdot y_2) = (z_1, z_2),$$

jollakin $(y_1, y_2) \in Q_1 \times Q_2$. Nyt yhtälölle on olemassa ratkaisu

$$(y_1, y_2) = (x_1 \backslash z_1, x_2 \backslash z_2),$$

missä \ on kvasiryhmien $(Q_1, \cdot)$ ja $(Q_2, \cdot)$ vasemmanpuoleinen jakolasku. Tämä pätee, sillä

$$\begin{aligned}(x_1, x_2) \cdot (x_1 \backslash z_1, x_2 \backslash z_2) &= (x_1 \cdot (x_1 \backslash z_1), x_2 \cdot (x_2 \backslash z_2)) \\ &= (z_1, z_2). \qquad \text{(lause 2.2.2, ominaisuus 1)}\end{aligned}$$

Tiedetään, että x_1, $z_1 \in Q_1$ ja x_2, $z_2 \in Q_2$. Vasemmanpuoleisen jakolaskun määritelmän 2.2.1 mukaan sen tulos on yksikäsitteinen ja kuuluu kvasiryhmään. Täten ratkaisu (y_1, y_2) on yksikäsitteinen ja kuuluu joukkoon $Q_1 \times Q_2$. On siis osoitettu, että $(Q_1 \times Q_2, \cdot)$ on kvasiryhmä.

Osoitetaan vielä, että kvasiryhmässä $(Q_1 \times Q_2, \cdot)$ vasemman- ja oikeanpuoleinen jakolasku ovat lauseessa esitetyt. Oletetaan ensin, että (x_1, x_2), (y_1, y_2) ja $(z_1, z_2) \in Q_1 \times Q_2$ ja että

$$(x_1, x_2)\backslash(y_1, y_2) = (z_1, z_2)$$

pätee. Toisin sanoen

$$(x_1, x_2) \cdot (z_1, z_2) = (x_1 \cdot z_1, x_2 \cdot z_2) = (y_1, y_2),$$

eli $y_1 = x_1 \cdot z_1$ ja $y_2 = x_2 \cdot z_2$. Koska alkiot x_1, y_1 ja $z_1 \in Q_1$ ja alkiot x_2, y_2 ja $z_2 \in Q_2$, niin vasemmanpuoleisen jakolaskun määritelmän 2.2.1 nojalla saadaan ratkaisu

$$(z_1, z_2) = (x_1\backslash y_1, x_2\backslash y_2).$$

Siis väite pätee vasemmanpuoleisen jakolaskun osalta.

Oletetaan vielä, että tiedetään alkiot (x_1, x_2), (y_1, y_2) ja $(z_1, z_2) \in Q_1 \times Q_2$, joille pätee

$$(x_1, x_2)/(y_1, y_2) = (z_1, z_2).$$

Tällöin

$$(z_1, z_2) \cdot (y_1, y_2) = (x_1, x_2),$$

eli $x_1 = z_1 \cdot y_1$ ja $x_2 = z_2 \cdot y_2$. Tiedetään, että alkiot x_1, y_1 ja $z_1 \in Q_1$ ja alkiot x_2, y_2 ja $z_2 \in Q_2$, joten oikeanpuoleisen jakolaskun määritelmän 2.2.2 nojalla voidaan päätellä, että ratkaisu on

$$(z_1, z_2) = (x_1/y_1, x_2/y_2).$$

Näin on osoitettu, että lause pätee myös oikeanpuoleisen jakolaskun kohdalla. □

Määritelmä 2.4.3 (vrt. [7, s. 300])**.** Olkoot $(Q_1, \cdot)$ ja $(Q_2, \cdot)$ kvasiryhmiä ja $(Q_1 \times Q_2, \cdot)$ kvasiryhmä, jossa kertolasku on määritelty

$$(x_1, x_2) \cdot (y_1, y_2) = (x_1 \cdot y_1, x_2 \cdot y_2),$$

kun x_1, $y_1 \in Q_1$ ja $x_2, y_2 \in Q_2$. Tällöin kvasiryhmää $(Q_1 \times Q_2, \cdot)$ kutsutaan *kvasiryhmien* $(Q_1, \cdot)$ *ja* $(Q_2, \cdot)$ *tuloksi.*

Esimerkki 2.4.2. Esimerkissä 2.1.1 osoitettiin struktuurin $(\mathbb{R}, -)$ olevan kvasiryhmä. Nyt määritelmän 2.4.3 nojalla myös $(\mathbb{R} \times \mathbb{R}, -)$ on kvasiryhmä, jossa laskutoimitus $-$ on määritelty

$$(x_1, x_2) - (y_1, y_2) = (x_1 - y_1, x_2 - y_2).$$

2.5 Homotopiat ja isotopiat

Määritelmä 2.5.1 (vrt. [7, s. 302])**.** Olkoot $(Q_1, \cdot)$ ja $(Q_2, *)$ kvasiryhmiä. Olkoon (f, g, h) järjestetty kolmikko, joka koostuu funktioista joukolta Q_1 joukkoon Q_2. Tällä tavoin muodostettua järjestettyä kolmikkoa kutsutaan *kvasiryhmän* $(Q_1, \cdot)$ *homotopiaksi kvasiryhmälle* $(Q_2, *)$, jos

$$f(x) * g(y) = h(x \cdot y) \qquad \forall x, y \in Q_1.$$

Tällöin funktioita f, g ja h kutsutaan *homotopian komponenteiksi.*

Määritelmä 2.5.2 (vrt. [7, s. 302])**.** Olkoot $(Q_1, \cdot)$ ja $(Q_2, *)$ kvasiryhmiä ja olkoon (f, g, h) kvasiryhmän $(Q_1, \cdot)$ homotopia kvasiryhmälle $(Q_2, *)$. Jos homotopian komponentit f, g ja h ovat bijektioita, niin homotopiaa kutsutaan *isotopiaksi.* Tällöin kvasiryhmien $(Q_1, \cdot)$ ja $(Q_2, *)$ sanotaan olevan *isotooppiset.*

Määritelmistä 2.4.1 ja 2.5.1 huomataan, että kun (f, g, h) on kvasiryhmähomotopia kvasiryhmältä $(Q_1, \cdot)$ kvasiryhmään $(Q_2, *)$, niin se on myös kvasiryhmähomomorfismi, jos $f = g = h$. Toisaalta nähdään myös, että kvasiryhmähomomorfismi $f : Q_1 \to Q_2$ muodostaa homotopian (f, f, f) kvasiryhmältä $(Q_1, \cdot)$ kvasiryhmään $(Q_2, *)$. [7, s. 303]

Esimerkki 2.5.1. Tarkastellaan struktuureja $(\mathbb{R}, +)$ ja $(\mathbb{R}, *)$, joissa $+$ on reaalilukujen yhteenlasku ja $*$ on esimerkissä 2.4.1 määritelty reaalilukujen aritmeettinen keskiarvo. Tiedetään, että $(\mathbb{R}, +)$ on ryhmä, joten lauseen 2.1.1 perusteella se on myös kvasiryhmä. Lisäksi esimerkissä 2.4.1 osoitettiin, että $(\mathbb{R}, *)$ on kvasiryhmä. Olkoot funktiot f, g, $h : \mathbb{R} \to \mathbb{R}$ määritelty siten, että $f : x \mapsto \frac{x}{2}$, $g : x \mapsto \frac{x}{2}$ ja $h : id_{\mathbb{R}}$. Osoitetaan, että (f, g, h) on kvasiryhmän $(\mathbb{R}, *)$ isotopia kvasiryhmälle $(\mathbb{R}, +)$. Olkoot x ja y reaalilukuja. Tällöin

$$\begin{aligned} f(x) + g(y) &= \frac{x}{2} + \frac{y}{2} \\ &= \frac{x + y}{2} \\ &= x * y \\ &= h(x * y). \end{aligned}$$

Lause 2.5.1 (vrt. [2, s. 561])**.** *Olkoot kvasiryhmät* $(Q_1, \cdot)$ *ja* $(Q_2, *)$ *isotooppiset ja olkoon* (f, g, h) *järjestetty kolmikko, joka koostuu funktioista joukolta* Q_1 *joukkoon* Q_2*. Olkoot lisäksi* x *ja* y *alkioita joukossa* Q_2*. Tällöin*

$$x * y = h(f^{-1}(x) \cdot g^{-1}(y)).$$

Todistus. Lause seuraa suoraan isotopian määritelmästä 2.5.2. □

Huomataan, että äärellisten kvasiryhmien ja isotopian avulla pystytään muodostamaan uusia kvasiryhmiä. Isotopiat ovat hyödyllisiä kvasiryhmien luomisessa, sillä n alkion kvasiryhmällä on jopa $(n!)^3$ isotopiaa. (Ks. [1, s. 122]).

Esimerkki 2.5.2. Olkoon joukko $Q = \{1, 2, 3, 4\}$ ja olkoon siinä määritelty kertolasku $\cdot$ seuraavasti:

$$\begin{aligned}
1 \cdot 1 &= 1,\\
1 \cdot 2 &= 2,\\
1 \cdot 3 &= 3,\\
1 \cdot 4 &= 4,\\
2 \cdot 1 &= 2,\\
2 \cdot 2 &= 1,\\
2 \cdot 3 &= 4,\\
2 \cdot 4 &= 3,\\
3 \cdot 1 &= 3,\\
3 \cdot 2 &= 4,\\
3 \cdot 3 &= 1,\\
3 \cdot 4 &= 2,\\
4 \cdot 1 &= 4,\\
4 \cdot 2 &= 3,\\
4 \cdot 3 &= 2,\\
4 \cdot 4 &= 1.
\end{aligned}$$

Nähdään, että selvästi $(Q, \cdot)$ on kvasiryhmä. Olkoot sitten

$$f = ((1, 4), (2, 1), (3, 2), (4, 3)),$$

$$g = ((1, 3), (2, 4), (3, 1), (4, 2))$$

ja

$$h = ((1, 4), (2, 3), (3, 1), (4, 2)).$$

Nyt voidaan määritellä kertolasku $*$ siten, että $(Q, *)$ on kvasiryhmä ja että (f, g, h) on kvasiryhmäisotopia kvasiryhmästä $(Q, \cdot)$ kvasiryhmään $(Q, *)$. Kertolaskun alkion $x * y$ laskemisessa käytetään lauseessa 2.5.1 esiintynyttä yhtälöä $x * y = h(f^{-1}(x) \cdot g^{-1}(y))$, kun $x, y \in Q$. Tällöin kertolaskuksi * saadaan

$$\begin{aligned}
1 * 1 &= h(f^{-1}(1) \cdot g^{-1}(1)) = h(2 \cdot 3) = h(4) = 2,\\
1 * 2 &= h(f^{-1}(1) \cdot g^{-1}(2)) = h(2 \cdot 4) = h(1) = 4,\\
1 * 3 &= h(f^{-1}(1) \cdot g^{-1}(3)) = h(2 \cdot 1) = h(2) = 3,\\
1 * 4 &= h(f^{-1}(1) \cdot g^{-1}(4)) = h(2 \cdot 2) = h(3) = 1,\\
2 * 1 &= h(f^{-1}(2) \cdot g^{-1}(1)) = h(3 \cdot 3) = h(1) = 4,\\
2 * 2 &= h(f^{-1}(2) \cdot g^{-1}(2)) = h(3 \cdot 4) = h(2) = 3,\\
2 * 3 &= h(f^{-1}(2) \cdot g^{-1}(3)) = h(3 \cdot 1) = h(3) = 1,\\
2 * 4 &= h(f^{-1}(2) \cdot g^{-1}(4)) = h(3 \cdot 2) = h(4) = 2,
\end{aligned}$$

$$
\begin{aligned}
3 * 1 &= h(f^{-1}(3) \cdot g^{-1}(1)) = h(4 \cdot 3) = h(2) = 3,\\
3 * 2 &= h(f^{-1}(3) \cdot g^{-1}(2)) = h(4 \cdot 4) = h(3) = 1,\\
3 * 3 &= h(f^{-1}(3) \cdot g^{-1}(3)) = h(4 \cdot 1) = h(4) = 2,\\
3 * 4 &= h(f^{-1}(3) \cdot g^{-1}(4)) = h(4 \cdot 2) = h(1) = 4,\\
4 * 1 &= h(f^{-1}(4) \cdot g^{-1}(1)) = h(1 \cdot 3) = h(3) = 1,\\
4 * 2 &= h(f^{-1}(4) \cdot g^{-1}(2)) = h(1 \cdot 4) = h(4) = 2,\\
4 * 3 &= h(f^{-1}(4) \cdot g^{-1}(3)) = h(1 \cdot 1) = h(1) = 4,\\
4 * 4 &= h(f^{-1}(4) \cdot g^{-1}(4)) = h(1 \cdot 2) = h(2) = 3,
\end{aligned}
$$

jolloin selvästi $(Q, *)$ on kvasiryhmä. Nähdään myös, että (f, g, h) on kvasiryhmäisotopia, sillä f, g ja h ovat bijektioita ja lisäksi kaikilla $x, y \in Q$ pätee

$$f(x) * g(y) = h(x \cdot y).$$

Tämä voidaan tarkistaa sijoittamalla kaikki alkioiden $\{1, 2, 3, 4\}$ kahden alkion yhdistelmät yhtälöön. Esimerkiksi jos $x = 1$ ja $y = 2$, niin

$$f(x) * g(y) = f(1) * g(2) = 4 * 4 = 3 = h(2) = h(1 \cdot 2) = h(x \cdot y).$$

Muut sijoitukset sivuutetaan tässä yhteydessä, mutta todetaan väitteen pätevän.

Apulause 2.5.2. *Olkoot $(Q_1, \cdot)$, $(Q_2, *)$ ja $(Q_3, +)$ kvasiryhmiä, joilla on kvasiryhmähomotopiat $(f, g, h) : Q_2 \to Q_3$ ja $(f', g', h') : Q_1 \to Q_2$. Tällöin $(f \circ f', g \circ g', h \circ h') : Q_1 \to Q_3$ on kvasiryhmähomomorfismi.*

Todistus. (Ks. [7, s. 303]). Olkoot x, $y \in Q_1$. Nyt homotopian määritelmästä saadaan

$$
\begin{aligned}
(f \circ f')(x) + (g \circ g')(y) &= f(f'(x)) + g(g'(y))\\
&= h(f'(x) * g'(y))\\
&= h(h'(x \cdot y))\\
&= (h \circ h')(x \cdot y),
\end{aligned}
$$

joten $(f \circ f', g \circ g', h \circ h')$ on kvasiryhmähomomorfismi joukolta Q_1 joukkoon Q_3. □

Seuraus 2.5.3. *Kvasiryhmien isotooppisuus on ekvivalenssirelaatio.*

Todistus. (Vrt. [7, s. 303]). Jotta voidaan osoittaa isotopian muodostavan ekvivalenssirelaation kvasiryhmien välille, tulee osoittaa että isotooppisuusrelaatio on reflektiivinen, transitiivinen ja symmetrinen. Identiteettikuvaus id_Q muodostaa kvasiryhmässä $(Q, \cdot)$ isotopian (id_Q, id_Q, id_Q), sillä id_Q on bijektiivinen ja selvästi homomorfismi, koska $id_Q(x) \cdot id_Q(x) = x \cdot x = id_Q(x \cdot x)$ kaikilla $x \in Q$. Täten isotooppisuusrelaatio on refleksiivinen.

Oletetaan sitten, että $(Q_1, \cdot)$, $(Q_2, *)$ ja $(Q_3, +)$ ovat kvasiryhmiä. Oletetaan lisäksi, että $(Q_1, \cdot)$ ja $(Q_2, *)$ ovat isotooppiset sekä että $(Q_2, *)$ ja $(Q_3, +)$ ovat isotooppiset. Nyt apulauseesta 2.5.2 seuraa, että isotopioiden yhdiste joukolta Q_1 joukkoon Q_3 on isotopia. Täten isotooppisuusrelaatio on transitiivinen.

Oletetaan viimeiseksi, että (f, g, h) on isotopia kvasiryhmästä $(Q_1, \cdot)$ kvasiryhmään $(Q_2, *)$. Tarkastellaan joukon Q_2 sellaisia alkioita x ja y, joille pätee $f(x') = x$ ja $g(y') = y$ joillain yksittäisillä x', $y' \in Q_1$. Tällöin kvasiryhmien isotopian määritelmästä 2.5.2 seuraa, että

$$h(x' \cdot y') = f(x') * g(y') = x * y.$$

Täten

$$h^{-1}(x * y) = x' \cdot y' = f^{-1}(x) \cdot g^{-1}(y),$$

jolloin nähdään, että (f^{-1}, g^{-1}, h^{-1}) on isotopia kvasiryhmältä $(Q_2, *)$ kvasiryhmään $(Q_1, \cdot)$. Isotooppisuusrelaatio on siis myös symmetrinen. Näin ollen on osoitettu, että isotooppisuusrelaatio on ekvivalenssirelaatio minkä tahansa kvasiryhmien välillä. □

2.6 Pääisotopiat

Määritelmä 2.6.1 (vrt. [7, s. 304])**.** Olkoot $(Q_1, \cdot)$ ja $(Q_1, *)$ kvasiryhmiä. Kvasiryhmäisotopiaa $(f, g, h) : Q_1 \to Q_1$ kutsutaan *pääisotopiaksi*, jos kolmas komponentti h on identiteettikuvaus $id_{Q_1} : Q_1 \to Q_1$. Tällöin kvasiryhmien $(Q_1, \cdot)$ ja $(Q_1, *)$ sanotaan olevan *pääisotooppiset*.

Esimerkki 2.6.1. Esimerkin 2.1.1 nojalla tiedetään, että $(\mathbb{R}, -)$ on kvasiryhmä. Toisaalta esimerkissä 2.5.1 todettiin, että myös $(\mathbb{R}, +)$ on kvasiryhmä. Osoitetaan, että kvasiryhmät ovat pääisotooppiset. Olkoot x ja y reaalilukuja. Olkoot lisäksi funktiot f, g ja h määritelty siten, että $f = id_{\mathbb{R}}$, $g : x \mapsto -x$ ja $h = id_{\mathbb{R}}$. Huomataan, että selvästi funktiot f, g ja h ovat bijektioita. Nyt lisäksi

$$f(x) + g(y) = x - y = h(x - y),$$

joten (f, g, h) on kvasiryhmien $(\mathbb{R}, -)$ ja $(\mathbb{R}, +)$ välinen isotopia, ja koska isotopian kolmas komponentti h on identiteettikuvaus $id_{\mathbb{R}}$, niin se on myös kvasiryhmien välinen pääisotopia.

Lause 2.6.1 (Vrt. [7, s. 304])**.** *Olkoot $(Q_1, *)$ ja $(Q_2, \cdot)$ kvasiryhmiä ja olkoon $(f, g, h) : Q_1 \to Q_2$ kvasiryhmäisotopia. Lisäksi olkoon $\bullet$ laskutoimitus, jossa*

$$x \bullet y = h^{-1}(h(x) \cdot h(y)), \qquad \forall x, y \in Q_1.$$

Tällöin seuraavat ominaisuudet pätevät:

1. *Struktuuri $(Q_1, \bullet)$ on kvasiryhmä.*

2. *On olemassa isomorfismi* $h : (Q_1, \bullet) \to (Q_2, \cdot)$.

3. *Isotopia* (f, g, h) *voidaan jakaa tekijöihin seuraavasti:*
   $(f, g, h) = (h, h, h) \circ (h^{-1} \circ f, h^{-1} \circ g, id_{Q_1})$.

   Toisin sanoen, isotopian (f, g, h) *tekijät ovat pääisotopia*
   $(h^{-1} \circ f, h^{-1} \circ g, id_{Q_1}) : (Q_1, *) \to (Q_1, \bullet)$ *ja isomorfismi h:* $(Q_1, \bullet) \to (Q_2, \cdot)$.

Todistus. Lauseen todistus on sivuutettu lähteessä [7], joten osoitetaan se tässä tutkielmassa todeksi. Tarkastellaan aluksi ensimmäistä väitettä. Oletetaan, että tunnetaan alkiot x, $y \in Q_1$. Tällöin $h(x)$ ja $h(y)$ ovat yksikäsitteisiä, koska h on funkio. Toisaalta koska $(Q_2, \cdot)$ on kvasiryhmä, niin sen alkioiden kertolaskun $h(x) \cdot h(y)$ tulos on yksikäsitteinen ja kuuluu joukkoon Q_2. Lisäksi funktion h bijektiivisyydestä seuraa, että myös sen käänteisfunktio h^{-1} on bijektio. Täten $h^{-1}(h(x) \cdot h(y))$ on yksikäsitteinen ja kuuluu joukkoon Q_1.

Oletetaan sitten, että tunnetaan alkiot x ja $z \in Q_1$, joille pätee

$$z = h^{-1}(h(x) \cdot h(y)) = x \bullet y,$$

jollakin $y \in Q_1$. Nähdään, että nyt pätee myös $h(z) = h(x) \cdot h(y)$, eli vasemmanpuoleisen jakolaskun määritelmän 2.2.1 nojalla $h(y) = h(x) \backslash h(z)$. Siis oltava $y = h^{-1}(h(x) \backslash h(z))$, sillä h on bijektio. Todetaan tämä vielä laskemalla

$$\begin{aligned}
x \bullet y &= x \bullet h^{-1}(h(x) \backslash h(z)) \\
&= h^{-1}(h(x) \cdot h(h^{-1}(h(x) \backslash h(z)))) \\
&= h^{-1}(h(x) \cdot (h(x) \backslash h(z))) \\
&= h^{-1}(h(z)) && \text{(lause 2.2.2, ominaisuus 1)} \\
&= z.
\end{aligned}$$

Osoitetaan vielä, että näin saatu y on yksikäsitteinen. Oletetaan, että on olemassa y ja $y' \in Q_1$, joille pätee $x \bullet y = x \bullet y'$. Nyt

$$\begin{aligned}
h^{-1}(h(x) \cdot h(y)) &= h^{-1}(h(x) \cdot h(y')), \\
h(x) \cdot h(y) &= h(x) \cdot h(y'), \\
h(y) &= h(y'),
\end{aligned}$$

mutta koska h on bijektiona injektio, niin tulee olla $y = y'$.

Oletetaan vielä, että tunnetaan sellaiset alkiot y ja $z \in Q_1$, joille pätee

$$z = h^{-1}(h(x) \cdot h(y)) = x \bullet y,$$

jollakin $x \in Q_1$. Tällöin oikeanpuoleisen jakolaskun määritelmän 2.2.2 nojalla $h(x) = h(z)/h(y)$. Nyt pätee, että $x = h^{-1}(h(z)/h(y))$, koska h on bijektio.

Todetaan tämä vielä laskemalla

$$\begin{aligned} x \bullet y &= h^{-1}(h(z)/h(y)) \bullet y, \\ &= h^{-1}(h(h^{-1}(h(z)/h(y))) \cdot h(y)), \\ &= h^{-1}((h(z)/h(y)) \cdot h(y)), \\ &= h^{-1}(h(z)) && \text{(lause 2.2.2, ominaisuus 2)} \\ &= z. \end{aligned}$$

Osoitetaan, että näin ratkaistu x on yksikäsitteinen. Oletetaan, että on olemassa x ja $x' \in Q_1$ siten, että pätee $x \bullet y = x' \bullet y$. Tällöin

$$\begin{aligned} h^{-1}(h(x) \cdot h(y)) &= h^{-1}(h(x') \cdot h(y)), \\ h(x) \cdot h(y) &= h(x') \cdot h(y), \\ h(x) &= h(x'), \end{aligned}$$

ja koska h on bijektiona injektio, niin täytyy olla $x = x'$. Täten on osoitettu, että $(Q_1, \bullet)$ on kvasiryhmä, eli lauseen väite 1 pätee.

Tarkastellaan seuraavaksi väitettä 2. Kvasiryhmäisotopian (f, g, h) komponentti $h : Q_1 \to Q_2$ on bijektio, joten sillä on olemassa käänteisfunkto $h^{-1} : Q_2 \to Q_1$. Käänteisfunktion määritelmästä tiedetään, että kaikilla $x' \in Q_2$ pätee $h(h^{-1}(x')) = x'$. Nyt kaikille x, $y \in Q_1$ pätee, että

$$h(x \bullet y) = h(h^{-1}(h(x) \cdot h(y))) = h(x) \cdot h(y),$$

joten h on isomorfismi kvasiryhmältä $(Q_1, \bullet)$ kvasiryhmään $(Q_2, \cdot)$, eli lauseen väite 2 pätee.

Viimeiseksi tarkastellaan väitettä 3. Käänteisfunktion määritelmästä seuraa, että $h \circ h^{-1} = id_{Q_2}$. Lisäksi identiteettifunktiolle pätee, että $h \circ id_{Q_1} = id_{Q_1} \circ h = h$. Yhdistettyjen funktioiden liitännäisyyden perustella siten pätee

$$f = id_{Q_2} \circ f = (h \circ h^{-1}) \circ f = h \circ (h^{-1} \circ f),$$

$$g = id_{Q_2} \circ g = (h \circ h^{-1}) \circ g = h \circ (h^{-1} \circ g)$$

ja

$$h = h \circ id_{Q_1}.$$

Väitteen 2 nojalla $h : (Q_1, \bullet) \to (Q_2, \cdot)$ on kvasiryhmäisomorfismi. Järjestetyn kolmikon $(h^{-1} \circ f, h^{-1} \circ g, id_{Q_1})$ lähtöjoukko on kvasiryhmä $(Q_1, *)$ ja maalijoukko on kvasiryhmä $(Q_1, \bullet)$, sillä funktiot f ja g on määritelty kvasiryhmältä $(Q_1, *)$ kvasiryhmään $(Q_2, \cdot)$, käänteisfunktio h^{-1} on määritelty kvasiryhmältä $(Q_2, \cdot)$ kvasiryhmään $(Q_1, \bullet)$ ja identiteettikuvaus id_{Q_1} on määritelty joukolta Q_1 joukkoon Q_1. Täten lauseen väite 3 pätee. □

2.7 Luupit

Ryhmäteoriasta tiedetään, että kaikilla ryhmillä on olemassa neutraalialkio. Myös kvasiryhmällä voi olla neutraalialkio ja tällöin kvasiryhmää kutsutaan luupiksi.

Määritelmä 2.7.1 (ks. [7, s. 306])**.** Kvasiryhmää $(Q, \cdot)$ kutsutaan *luupiksi*, jos se sisältää sellaisen alkion e, jolle pätee

$$e \cdot x = x = x \cdot e, \qquad \text{kaikilla } x \in Q.$$

Tällaista joukon Q alkiota e kutsutaan *luupin* $(Q, \cdot, e)$ *neutraalialkioksi.*

Huomataan, että kaikki ryhmät ovat liitännäisiä luuppeja. Esimerkissä 3.2.3 tullaan osoittamaan, että on olemassa myös ei-liitännäisiä luuppeja.

Lause 2.7.1. *Olkoon $(Q, \cdot)$ epätyhjä kvasiryhmä, jossa on määritelty vasemmanpuoleinen jakolasku $\backslash$ ja oikeanpuoleinen jakolasku $/$. Olkoot lisäksi a ja b joukon Q alkioita. Määritellään uusi operaatio $*$ joukossa Q seuraavasti:*

$$x * y = (x/b) \cdot (a\backslash y), \qquad \textit{kun } x, y \in Q.$$

Tällöin $(Q, *, a \cdot b)$ on luuppi, joka on pääisotooppinen kvasiryhmän $(Q, \cdot)$ kanssa.

Todistus. (Vrt. [7, s. 308]). Olkoon z sellainen kvasiryhmän $(Q, \cdot)$ alkio, jolle pätee

$$x * y = (x/b) \cdot (a\backslash y) = z.$$

Osoitetaan aluksi, että $(Q, *)$ on kvasiryhmä.Lähteessä [7] kvasiryhmäksi osoittaminen on sivuutettu, mutta esitetään se tässä tutkielmassa todistuksen selkeyttämiseksi. Oletetaan, että alkiot x ja y tunnetaan. Koska $(Q, \cdot)$ on kvasiryhmä, niin se on suljettu vasemman- ja oikeanpuoleisen jakolaskun suhteen ja niiden tulokset ovat yksikäsitteisiä. Täten on olemassa yksikäsitteiset x/b, $a\backslash y \in Q$. Toisaalta edelleen koska $(Q, \cdot)$ on kvasiryhmä, niin myös sen alkioiden kertolaskun tulos on yksikäsitteinen ja kuuluu joukkoon Q. Täten $z = (x/b) \cdot (a\backslash y)$ on määritelty yksikäsitteisesti ja kuuluu joukkoon Q.

Oletetaan sitten, että alkiot x, $z \in Q$ tunnetaan. Nyt vasemmanpuoleisen jakolaskun määritelmästä 2.2.1 saadaan, että $a\backslash y = (x/b)\backslash z$. Käyttämällä vasemmanpuoleisen jakolaskun määritelmää uudestaan saadaan ratkaisu

$$y = a \cdot ((x/b)\backslash z).$$

Nyt selvästi $y \in Q$, mutta tulee vielä osoittaa, että ratkaisu on yksikäsitteinen. Oletetaan, että on olemassa sellainen alkio $y' \in Q$, jolle $x * y' = z$. Nyt

$$\begin{aligned}
y &= a \cdot ((x/b)\backslash z) \\
&= a \cdot ((x/b)\backslash (x * y')) \\
&= a \cdot ((x/b)\backslash ((x/b) \cdot (a\backslash y'))) \\
&= a \cdot (a\backslash y') && \text{(lause 2.2.2, ominaisuus 3)} \\
&= y', && \text{(lause 2.2.2, ominaisuus 1),}
\end{aligned}$$

eli saatu ratkaisu y on yksikäsitteinen.

Oletetaan sitten, että alkiot y ja z tunnetaan. Nyt oikeanpuoleisen jakolaskun määritelmästä 2.2.2 saadaan, että $x/b = z/(a\backslash y)$, eli

$$x = (z/(a\backslash y)) \cdot b.$$

Osoitetaan, että näin saatu ratkaisu $x \in Q$ on yksikäsitteinen. Oletetaan, että on olemassa sellainen $x' \in Q$, jolle $x' * y = z$. Tällöin

$$\begin{aligned}
x &= (z/(a\backslash y)) \cdot b \\
&= ((x' * y)/(a\backslash y)) \cdot b \\
&= (((x'/b) \cdot (a\backslash y))/(a\backslash y)) \cdot b \\
&= (x'/b) \cdot b && \text{(lause 2.2.2, ominaisuus 4)} \\
&= x', && \text{(lause 2.2.2, ominaisuus 2)}
\end{aligned}$$

joten saatu ratkaisu x on yksikäsitteinen. Täten on osoitettu, että $(Q, *)$ on kvasiryhmä.

Osoitetaan seuraavaksi, että $a \cdot b$ on kvasiryhmän $(Q, *)$ neutraalialkio. Nyt kaikille $x \in Q$ pätee

$$\begin{aligned}
x * (a \cdot b) &= (x/b) \cdot (a\backslash(a \cdot b)) \\
&= (x/b) \cdot b && \text{(lause 2.2.2, ominaisuus 3)} \\
&= x. && \text{(lause 2.2.2, ominaisuus 2)}
\end{aligned}$$

Lisäksi pätee

$$\begin{aligned}
(a \cdot b) * x &= ((a \cdot b)/b) \cdot (a\backslash x) \\
&= a \cdot (a\backslash x) && \text{(lause 2.2.2, ominaisuus 4)} \\
&= x. && \text{(lause 2.2.2, ominaisuus 1)}
\end{aligned}$$

Täten on osoitettu, että $a \cdot b$ on kvasiryhmän $(Q, *)$ neutraalialkio, eli $(Q, *, a \cdot b)$ on luuppi.

Osoitetaan vielä, että on olemassa pääisotopia kvasiryhmältä $(Q, \cdot)$ luuppiin $(Q, *, a \cdot b)$. Määritellään funktiot $f, g : Q \to Q$ siten, että $f : x \mapsto x \cdot b$ ja $g : x \mapsto a \cdot x$. Tulee osoittaa, että f ja g ovat bijektioita. Olkoon x' sellainen alkio joukossa Q, jolle pätee $x \neq x'$. Nyt

$$f(x) = x \cdot b \neq x' \cdot b = f(x'),$$

sillä $(Q, \cdot)$ on kvasiryhmä. Niin ikään

$$g(x) = a \cdot x \neq a \cdot x' = g(x'),$$

koska $(Q, \cdot)$ on kvasiryhmä. Siis f ja g ovat injektioita. Valitaan sitten $z \in Q$. Koska $(Q, \cdot)$ on kvasiryhmä, on olemassa sellaiset alkiot x, $x' \in Q$, että $a \cdot x = z$

ja $x' \cdot b = z$, eli $g(x) = z$ js $f(x') = z$. Täten f ja g ovat myös surjektioita. Täten siis f ja g ovat bijektioita ja koska lisäksi kaikilla x, $y \in Q$ pätee

$$\begin{aligned} f(x) * g(y) &= (x \cdot b) * (a \cdot y) \\ &= ((x \cdot b)/b) \cdot (a\backslash(a \cdot y)) \\ &= x \cdot (a\backslash(a \cdot y)) && \text{(lause 2.2.2, ominaisuus 4)} \\ &= x \cdot y, && \text{(lause 2.2.2, ominaisuus 3)} \end{aligned}$$

niin $(f, g, id_Q) : (Q, \cdot) \to (Q, *)$ on pääisotopia kvasiryhmältä $(Q, \cdot)$ luuppiin $(Q, *, a \cdot b)$. □

Seuraavasta lauseesta ja sen seurauksesta huomataan, miksei ryhmäteoriassa käsitellä isotopiaa.

Lause 2.7.2. *Jos luuppi ja ryhmä ovat isotooppiset, niin ne ovat myös isomorfiset.*

Todistus. (Vrt. [7, s. 308]). Todistuksessa riittää tarkastella pääisotopian tapausta, sillä pääisotopian määritelmän 2.6.1 nojalla pääisotooppiset kvasiryhmät ovat myös isotooppisia keskenään. Olkoot $(Q, *, e_*)$ luuppi ja $(Q, \cdot, e_\bullet)$ ryhmä ja olkoot ne pääisotooppisia keskenään. Olkoon $(f, g, id_Q) : (Q, *, e_*) \to (Q, \cdot, e_\bullet)$ tämä pääisotopia. Tällöin siis kaikille joukon Q alkioille x, y pätee

$$f(x) \cdot g(y) = x * y.$$

Kun valitaan $y = e_*$, edellisestä yhtälöstä saadaan

$$f(x) \cdot g(e_*) = x * e_* = x.$$

Merkitään luvun $g(e_*)$ käänteislukua ryhmässä $(Q, \cdot, e_\bullet)$ merkinnällä $g(e_*)^{-1}$. Kun edellinen yhtälö kerrotaan puolittain ryhmän $(Q, \cdot, e_\bullet)$ kertolaskulla $\cdot$ oikealta luvulla $g(e_*)^{-1}$ saadaan

$$\begin{aligned} (f(x) \cdot g(e_*)) \cdot g(e_*)^{-1} &= x \cdot g(e_*)^{-1}, \\ f(x) \cdot (g(e_*) \cdot g(e_*)^{-1}) &= x \cdot g(e_*)^{-1}, \\ f(x) \cdot e_\bullet &= x \cdot g(e_*)^{-1} \\ f(x) &= x \cdot g(e_*)^{-1}. \end{aligned}$$

Toisaalta voidaan valita $x = e_*$, jolloin yhtälöstä $f(x) \cdot g(y) = x * y$ tulee

$$f(e_*) \cdot g(y) = e_* * y = y.$$

Edelleen kun edellinen yhtälö kerrotaan puolittain ryhmän $(Q, \cdot, e_\bullet)$ kertolaskulla $\cdot$ vasemmalta luvun $f(e_*)$ käänteisluvulla $f(e_*)^{-1}$ saadaan

$$\begin{aligned} f(e_*)^{-1} \cdot (f(e_*) \cdot g(y)) &= f(e_*)^{-1} \cdot y, \\ (f(e_*)^{-1} \cdot f(e_*)) \cdot g(y) &= f(e_*)^{-1} \cdot y, \\ e_\bullet \cdot g(y) &= f(e_*)^{-1} \cdot y, \\ g(y) &= f(e_*)^{-1} \cdot y. \end{aligned}$$

Nyt sijoittamalla saadut $f(x)$ ja $g(y)$ yhtälöön $f(x) \cdot g(y) = x * y$, saadaan

$$(x \cdot g(e_*)^{-1}) \cdot (f(e_*)^{-1} \cdot y) = x * y.$$

Kun edellinen yhtälö kerrotaan puolittain ryhmän $(Q, \cdot, e_\bullet)$ kertolaskulla $\cdot$ vasemmalta luvulla $f(e_*)^{-1}$ saadaan

$$f(e_*)^{-1} \cdot ((x \cdot g(e_*)^{-1}) \cdot (f(e_*)^{-1} \cdot y)) = f(e_*)^{-1} \cdot (x * y).$$

Kerrotaan edellinen yhtälö vielä puolittain ryhmän $(Q, \cdot, e_\bullet)$ kertolaskulla $\cdot$ oikealta luvulla $g(e_*)^{-1}$, jolloin pätee

$$(f(e_*)^{-1} \cdot ((x \cdot g(e_*)^{-1}) \cdot (f(e_*)^{-1} \cdot y))) \cdot g(e_*)^{-1} = (f(e_*)^{-1} \cdot (x * y)) \cdot g(e_*)^{-1}.$$

Koska $(Q, \cdot, e_\bullet)$ on ryhmä, sen kertolasku $\cdot$ on liitännäinen. Näin ollen edellisestä yhtälöstä saadaan

$$f(e_*)^{-1} \cdot x \cdot g(e_*)^{-1} \cdot f(e_*)^{-1} \cdot y \cdot g(e_*)^{-1} = f(e_*)^{-1} \cdot (x * y) \cdot g(e_*)^{-1}. \tag{1}$$

Tarkastellaan kuvausta $h : Q \to Q$, jolle pätee

$$h(x) = f(e_*)^{-1} \cdot x \cdot g(e_*)^{-1}.$$

Nyt yhtälö (1) voidaan kirjoittaa muodossa

$$h(x) \cdot h(y) = h(x * y),$$

eli $h : (Q, *, e_*) \to (Q, \cdot, e_\bullet)$ on homomorfia.

Osoitetaan vielä, että h on bijektio. Tiedetään, että funktio on bijektio, jos ja vain jos se on kääntyvä. Riittää siis osoittaa, että on olemassa käänteisfunktio h^{-1} siten, että $h \circ h^{-1} = id_Q = h^{-1} \circ h$. Olkoon $h' : Q \to Q$ funktio, jolle pätee $h' : x \mapsto f(e_*) \cdot x \cdot g(e_*)$. Osoitetaan, että h' on funktion h käänteisfunktio h^{-1}. Tämä pätee, sillä

$$\begin{aligned}
(h \circ h')(x) &= h(h'(x)) \\
&= h(f(e_*) \cdot x \cdot g(e_*)) \\
&= f(e_*)^{-1} \cdot (f(e_*) \cdot x \cdot g(e_*)) \cdot g(e_*)^{-1} \\
&= f(e_*)^{-1} \cdot f(e_*) \cdot x \cdot g(e_*) \cdot g(e_*)^{-1} \\
&= e_\bullet \cdot x \cdot e_\bullet \\
&= x.
\end{aligned}$$

ja koska lisäksi pätee

$$\begin{aligned}
(h' \circ h)(x) &= h'(h(x)) \\
&= h'(f(e_*)^{-1} \cdot x \cdot g(e_*)^{-1}) \\
&= f(e_*) \cdot (f(e_*)^{-1} \cdot x \cdot g(e_*)^{-1}) \cdot g(e_*) \\
&= f(e_*) \cdot f(e_*)^{-1} \cdot x \cdot g(e_*)^{-1} \cdot g(e_*) \\
&= e_\bullet \cdot x \cdot e_\bullet \\
&= x.
\end{aligned}$$

On siis osoitettu, että homomorfismi h on bijektio ja täten isomorfismi luupista $(Q, *, e_*)$ ryhmään $(Q, \cdot, e_\bullet)$. □

Seuraus 2.7.3. *Jos kaksi ryhmää ovat isotooppiset, ne ovat myös isomorfiset.*

3 Latinalaiset neliöt

Esimerkissä 2.5.2 kvasiryhmä $(\{1,2,3,4\},\cdot)$ esitettiin sen kertolaskun $\cdot$ määritelmän avulla. Tässä luvussa esitellään latinalaiset neliöt ja niiden yhteys kvasiryhmien kertotauluihin, joiden avulla kvasiryhmät voi esittää tiiviimmällä tavalla.

3.1 Latinalaisten neliöiden määritelmä

Määritelmä 3.1.1 (vrt. [2, s. 559])**.** Olkoon L $n\times n$ -neliömatriisi, jonka alkiot kuuluvat joukkoon $Q = \{1,2,\ldots,n\}$. Jos kukin joukon Q alkioista esiintyy matriisin jokaisella rivillä ja jokaisessa sarakkeessa täsmälleen kerran, niin matriisia L kutsutaan *latinalaiseksi neliöksi*. Lukua n kutsutaan tällöin latinalaisen neliön L *kertaluvuksi*. Latinalaisen neliön sanotaan olevan *supistettu*, jos sen ensimmäinen rivi ja ensimmäinen sarake ovat luonnollisessa järjestyksessä.

Esimerkki 3.1.1. Olkoon $Q = \{1,2,3,4\}$. Joukon Q alkioista voidaan muodostaa kertaluvun 4 supistettu latinalainen neliö L taulukon 3.1 mukaisesti.

1	2	3	4
2	3	4	1
3	4	1	2
4	1	2	3

Taulukko 3.1: supistettu latinalainen neliö L

Huomautus 3.1.1. Kertalukua n olevien latinalaisten neliöiden tarkkaa lukumäärää ei tiedetä, kun $n > 10$. Vaikka tarkkoja lukumääriä ei tiedetä, on kuitenkin olemassa arvioita niiden suuruusluokista. Erään arvion mukaan kertaluvun 256 latinalaisia neliöitä on vähintään $3,05\cdot 10^{101723}$ ja enintään $7,53\cdot 10^{102804}$. Arviossa käytettiin seuraavaa epäyhtälöä:

$$\frac{(n!)^{2n}}{n^{n^2}} \leq L(256) \leq \prod_{k=1}^{n} (k!)^{\frac{n}{k}}.$$

Todistus. Ks. [8, s. 186 - 187]. □

3.2 Latinalaisten neliöiden yhteys kvasiryhmiin

Kvasiryhmän kertotaulu kuvastaa kertolaskun toimintaa siten, että mikäli kvasiryhmän alkioille x, y ja z pätee, että $x\cdot y = z$, niin kertotaulusta alkion x nimeämältä riviltä alkion y nimeämästä sarakkeesta löytyy kertolaskun tulos z.

Esimerkki 3.2.1. Esitetään esimerkin 2.5.2 kvasiryhmän $(\{1,2,3,4\},\cdot)$ ja esimerkissä luodun kvasiryhmän $(\{1,2,3,4\},*)$ kertotaulut taulukoissa 3.2 ja 3.3.

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	1	4	3
3	3	4	1	2
4	4	3	2	1

Taulukko 3.2: kvasiryhmän $(Q,\cdot)$ kertotaulu

$*$	1	2	3	4
1	2	4	3	1
2	4	3	1	2
3	3	1	2	4
4	1	2	4	3

Taulukko 3.3: kvasiryhmän $(Q,*)$ kertotaulu.

Latinalaisten neliöiden yhteys kvasiryhmiin on helppo nähdä. Latinalaisesta neliöstä saadaan kvasiryhmän kertotaulu nimeämällä rivit ja sarakkeet sopivasti.

Lause 3.2.1. *Äärellinen epätyhjä joukko Q, jossa on määritelty kertolasku $\cdot$, muodostaa kvasiryhmän $(Q,\cdot)$, jos ja vain jos struktuurin $(Q,\cdot)$ kertotaulun sisältö on latinalainen neliö.*

Todistus. (Vrt. [7, s. 290]). Olkoon $(Q,\cdot)$ äärellinen kvasiryhmä, ja olkoot x ja y joukon Q alkioita. Tarkastellaan kvasiryhmän kertotaulun riviä, joka on nimetty alkion x mukaan. Nyt z esiintyy kertotaulussa alkion x nimeämällä rivillä alkion y nimeämässä sarakkeessa, jos ja vain jos

$$x \cdot y = z.$$

Koska $(Q,\cdot)$ on kvasiryhmä, niin kertolaskun tulos z on joukon Q alkio ja se on yksikäsitteinen. Tästä seuraa, että alkio z esiintyy alkion x nimeämällä rivillä ainoastaan alkion y nimeämässä sarakkeessa. Voidaan siis sanoa, että kukin joukon Q alkio esiintyy kertotaulun rivillä täsmälleen kerran. Vastaavalla päättelyllä voidaan osoittaa, että kukin joukon Q alkio esiintyy kullakin kertotaulun sarakkeella täsmälleen kerran. Näin ollen kvasiryhmän kertotaulun sisältö muodostaa latinalaisen neliön.

Olkoon sitten $Q = \{x_1, x_2, \ldots, x_n\}$ joukko, jossa on määritelty kertolasku $\cdot$. Tarkastellaan struktuurin $(Q,\cdot)$ kertotaulua, jossa rivit ja sarakkeet on nimetty joukon Q alkioiden $x_1, x_2, \ldots, x_n$ mukaisesti järjestyksessä. Oletetaan, että tämän kertotaulun sisältö on latinalainen neliö. Huomataan, että kertotaulun

alkio, joka on joukon Q alkion x_i nimeämällä rivillä ja alkion x_j nimeämällä sarakkeella, on $x_i \cdot x_j$, kun $1 \leq i, j \leq n$. Oletetaan, että yhtälö

$$x_i \cdot x_j = x_k$$

pätee struktuurissa $(Q, \cdot)$ ja että $1 \leq i, j, k \leq n$. Jos x_i ja x_j tiedetään, niin x_k voidaan laskea yksikäsitteisesti joukossa Q määritellyn kertolaskun $\cdot$ avulla. Oletetaan sitten, että tiedetään alkiot x_i ja x_k. Tarkastellaan alkion x_i nimeämää kertotaulun riviä. Koska kertotaulun sisältö on latinalainen neliö, tiedetään alkion x_k esiintyvän rivillä täsmälleen kerran. Olkoon se sarake, jossa x_k esiintyy, nimetty alkion x_j mukaan. Täten x_j on yksikäsitteinen ratkaisu yhtälölle $x_i \cdot x_j = x_k$ joukossa Q. Oletetaan vielä, että tiedetään alkiot x_j ja x_k. Tarkastellaan alkion x_j nimeämää kertotaulun saraketta. Edelleen tiedetään alkion x_k esiintyvän sarakkeessa täsmälleen kerran, koska kertotaulun sisältö on latinalainen neliö. Nyt se alkio x_i, joka nimeää rivin, jossa x_k esiintyy, on yhtälön $x_i \cdot x_j = x_k$ yksikäsitteinen ratkaisu joukossa Q. Täten on osoitettu, että $(Q, \cdot)$ on kvasiryhmä. □

Esimerkki 3.2.2. Olkoon Q joukko $\{1, 2, 3, 4\}$ ja olkoon L taulukon 3.4 mukainen kertaluvun 4 latinalainen neliö.

1	2	3	4
2	1	4	3
3	4	1	2
4	3	2	1

Taulukko 3.4: latinalainen neliö L

Nyt latinalaisesta neliöstä L voidaan muodostaa kvasiryhmän $(Q, \cdot)$ kertotaulu nimeämällä rivit ja sarakkeet taulukon 3.5 mukaisesti.

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	1	4	3
3	3	4	1	2
4	4	3	2	1

Taulukko 3.5: kvasiryhmän $(Q, \cdot)$ kertotaulu

Lause 3.2.2. *Olkoon Q äärellinen joukko. Tällöin kvasiryhmillä $(Q, \cdot)$ ja $(Q, *)$ on niiden kertotaulujen sisältönä sama latinalainen neliö L, jos ja vain jos niiden välillä on pääisotopia $(f, g, id_Q) : (Q, \cdot) \to (Q, *)$.*

Todistus. (Ks. [7, s. 305]). Olkoon $Q = \{x_1, x_2, \ldots, x_n\}$. Oletetaan ensin, että on olemassa kvasiryhmät $(Q, \cdot)$ ja $(Q, *)$, joilla on sama latinalainen neliö L niiden kertotaulujen sisältönä. On siis olemassa permutaatiot a, b, a' ja b' joukossa Q siten, että kvasiryhmien $(Q, \cdot)$ ja $(Q, *)$ kertotaulut ovat taulukoiden 3.6 ja 3.7 mukaiset.

$\cdot$	$a(x_1)$	$a(x_2)$	$\cdots$	$a(x_n)$
$b(x_1)$				
$b(x_2)$			L	
$\vdots$				
$b(x_n)$				

Taulukko 3.6: kvasiryhmän $(Q, \cdot)$ kertotaulu

$*$	$a'(x_1)$	$a'(x_2)$	$\cdots$	$a'(x_n)$
$b'(x_1)$				
$b'(x_2)$			L	
$\vdots$				
$b'(x_n)$				

Taulukko 3.7: kvasiryhmän $(Q, *)$ kertotaulu.

Nyt joukon Q alkioille y ja y' pätee

$$a'(y) * b'(y') = a(y) \cdot b(y').$$

Jos merkitään $y = a^{-1}(x)$ ja $y' = b^{-1}(x')$, missä x, $x' \in Q$, niin saadaan

$$\begin{aligned} a'(a^{-1}(x)) * b'(b^{-1}(x')) &= a(a^{-1}(x)) \cdot b(b^{-1}(x')) \\ &= x \cdot x' \end{aligned}$$

Jos lisäksi määritellään uudet funktiot f ja g siten, että $f = a' \circ a^{-1}$ ja $g = b' \circ b^{-1}$, niin

$$f(x) * g(x') = x \cdot x'.$$

Funktiot f ja g ovat permutaatioiden yhdistettyinä funktioina bijektioita, joten on osoitettu, että (f, g, id_Q) on pääisotopia kvasiryhmästä $(Q, \cdot)$ kvasiryhmään $(Q, *)$.

Oletetaan sitten, että on olemassa pääisotopia (f, g, id_Q) kvasiryhmästä $(Q, \cdot)$ kvasiryhmään $(Q, *)$. Tällöin $f(x) * g(x') = x \cdot x'$ kaikilla joukon Q alkioilla x ja x'. Olkoon L latinalainen neliö, joka muodostaa kvasiryhmän $(Q, \cdot)$ kertotaulun sisällön taulukon 3.8 kuvaamalla tavalla.

$\cdot$	x_1	x_2	$\cdots$	x_n
x_1				
x_2			L	
$\vdots$				
x_n				

Taulukko 3.8: kvasiryhmän $(Q, \cdot)$ kertotaulu

Kvasiryhmän $(Q, *)$ kertotaulun muodostamisessa on huomioitava, että $f(x) * g(x') = x \cdot x'$, jolloin saadaan taulukon 3.9 mukainen kertotaulu.

$*$	$g(x_1)$	$g(x_2)$	$\cdots$	$g(x_n)$
$f(x_1)$				
$f(x_2)$			L	
$\vdots$				
$f(x_n)$				

Taulukko 3.9: kvasiryhmän $(Q, *)$ kertotaulu.

Nähdään, että kvasiryhmillä $(Q, \cdot)$ ja $(Q, *)$ on sama latinalainen neliö kertotaulujensa sisältöinä. □

Lause 3.2.3. *Olkoon Q äärellinen epätyhjä joukko. Olkoon L latinalainen neliö, jonka alkiot ovat joukon Q alkioita. Tällöin on olemassa sellainen luuppi $(Q, \cdot, e)$, jonka kertotaulun sisältö on L.*

Todistus. (Ks. [7, s. 307]). Olkoon L taulukon 3.10 kuvailema latinalainen neliö.

x_{11}	x_{12}	$\cdots$	x_{1n}
x_{21}	x_{22}	$\cdots$	x_{2n}
$\vdots$	$\vdots$	$\ddots$	$\vdots$
x_{n1}	x_{n2}	$\cdots$	x_{nn}

Taulukko 3.10: Latinalainen neliö L

Silloin Q on sellainen n alkion joukko, jolle pätee $Q = \{x_{11}, x_{21}, \ldots, x_{n1}\} = \{x_{11}, x_{12}, \ldots, x_{1n}\}$. Tällöin taulukossa 3.11 esitetty latinalaisen neliön L reunustettu versio on luupin $(Q, \cdot, x_{11})$ kertotaulu.

$\cdot$	x_{11}	x_{12}	$\cdots$	x_{1n}
x_{11}	x_{11}	x_{12}	$\cdots$	x_{1n}
x_{21}	x_{21}	x_{22}	$\cdots$	x_{2n}
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
x_{n1}	x_{n1}	x_{n2}	$\cdots$	x_{nn}

Taulukko 3.11: luupin $(Q, \cdot, x_{11})$ kertotaulu

□

Esimerkki 3.2.3. Olkoon joukko $Q = \{1, 2, 3, 4, 5\}$ ja olkoon L taulukossa 3.12 esitetty latinalainen neliö.

1	2	3	4	5
2	1	4	5	3
3	5	1	2	4
4	3	5	1	2
5	4	2	3	1

Taulukko 3.12: latinalainen neliö L

Nyt lauseen 3.2.3 mukaan on olemassa luuppi $(Q, \cdot, 1)$, jonka kertotaulu on taulukon 3.13 mukainen.

$\cdot$	1	2	3	4	5
1	1	2	3	4	5
2	2	1	4	5	3
3	3	5	1	2	4
4	4	3	5	1	2
5	5	4	2	3	1

.

Taulukko 3.13: luupin $(Q, \cdot, 1)$ kertotaulu

Huomataan, että luuppi ei ole liitännäinen, sillä esimerkiksi

$$3 \cdot (3 \cdot 4) = 3 \cdot 2 = 5 \neq 4 = 1 \cdot 4 = (3 \cdot 3) \cdot 4.$$

Näin ollen on siis olemassa luuppeja, jotka eivät ole liitännäisiä.

Nyt voidaan vastata seuraavaan kysymykseen: Voiko kvasiryhmien tarkastelun palauttaa ryhmien tarkasteluksi? Kysymys voidaan muotoilla myös näin: voiko latinalaisen neliön rivit ja sarakkeet nimetä siten, että siitä tulee ryhmän kertotaulu, eli onko jokainen kvasiryhmä isomorfinen jonkin ryhmän kanssa? Seurataan kysymyksen vastauksessa lähteen [7, s. 310] päättelyä. Lauseesta 3.2.2 seuraa, että väite pätee, mikäli jokainen äärellinen kvasiryhmä on pääisotooppinen jonkin ryhmän kanssa. Toisaalta seurauksessa 2.5.3 osoitettiin, että isotopia on transitiivinen relaatio. Nyt koska lauseessa 2.7.1 todettiin, että jokaiselle kvasiryhmälle on olemassa luuppi siten, että ne ovat pääisotooppiset, niin riittää tarkastella tilannetta, ovatko luupit pääisotooppisia jonkin ryhmän kanssa. Lauseessa 2.7.2 osoitettiin, että jos luuppi on isotooppinen ryhmän kanssa, niin se on myös isomorfinen saman ryhmän kanssa. Kuitenkin esimerkissä 3.2.3 osoitettiin, että on olemassa ei-liitännäisiä luuppeja ja koska lauseen 2.4.1 mukaan isomorfisuus säilyttää liitännäisyyden, niin on olemassa kvasiryhmiä, jotka eivät ole isomorfisia minkään ryhmän kanssa. Täten voidaan todeta, että kvasiryhmien tarkastelu ryhmistä erillisenä algebrallisena struktuurina on mielekästä.

4 Kvasiryhmien kryptografinen sovellus

4.1 Kryptografiasta

Kryptografia tutkii tavallisen tekstin muuttamista salattuun muotoon salausalgoritmilla sekä salatun tekstin muuttamista takaisin tavalliseksi, eli selkotekstiksi. Salauksille kolme tärkeää ominaisuutta ovat yksityisyys, autenttisuus ja luotettavuus. Tässä yhteydessä yksityisyydellä tarkoitetaan sitä, että kenenkään ei-toivotun henkilön ei tule päästä käsiksi salauksen viesteihin. Autenttisuudella tarkoitetaan sitä, että viestin lähettäjä pystytään varmistamaan. Luotettavuus viittaa luottamukseen siitä, ettei viesti muutu vahingossa tai tarkoituksella sen välityksen aikana. Ihanteellinen salaus toteuttaisi kaikki kolme ominaisuutta, mutta valitettavasti joitain myönnytyksiä joudutaan usein tekemään esimerkiksi salattavan datan suuren määrän takia. [4, s. 175]

Salausalgoritmit voidaan määritellä niissä salaukseen ja salauksen purkamiseen käytettyjen matemaattisten operaatioiden kautta. Tällöin voidaan ajatella salausalgoritmien jakautuvan kahteen eri tyyppiin:

1. Algoritmit, joissa käytetään *julkista avainta*
2. Algoritmit, joissa käytetään *salaista avainta*.

Julkista avainta käyttäviä algoritmeja kutsutaan myös *epäsymmetrisiksi*. Epäsymmetriset salausalgoritmit käyttävät julkista avainta viestin salaamiseen ja salaista avainta viestin salauksen purkamiseen. Salaisen avaimen salausalgoritmit ovat vastaavasti toiselta nimeltään *symmetrisiä*. Symmetrisissä salausalgoritmeissä salaukseen käytetty avain voidaan laskea purkamiseen käytettävän avaimen avulla. Symmetristen salausalgoritmien luotettavuus perustuu siis sen avainten luotettavuuteen, koska avaimen paljastumisesta seuraisi se, että kuka tahansa pystyisi salaamaan ja purkamaan salattuja viestejä. Symmetriset salaussalausalgoritmit voidaan jakaa vielä kahteen kategoriaan: *lohkosalauksiin* (engl. block cipher) ja *jonosalauksiin* (engl. stream cipher). Lohko- ja jonosalaukset eroavat toisistaan siten, että lohkosalauksissa salattavasta viestistä muodostetaan lohkoja, jotka salataan kokonaisuutena, kun taas jonosalauksissa jokainen viestin alkio salataan itsenäisesti. [4, s. 176] Tässä luvussa esitellään symmetrinen jonosalausalgoritmi, joka käyttää salauksessa apunaan kvasiryhmiä.

4.2 Kvasiryhmiä soveltava salausalgoritmi

Määritelmä 4.2.1 (vrt. [3, s. 159])**.** Olkoon $Q = \{a_1, a_2, \ldots, a_n\}$ äärellinen joukko ja olkoon $(Q, *, \backslash)$ kvasiryhmä. Olkoon lisäksi Q^+ joukko epätyhjiä sanoja, jotka voidaan muodostaa joukon Q alkioista. Olkoot vielä $u_i, v_i \in A$ ja olkoon $k \geq 1$. Tällöin voidaan määritellä funktiot $f_* : Q^+ \to Q^+$ ja $f_\backslash : Q^+ \to Q^+$

seuraavasti:

$$f_*(u_1u_2\cdots u_k) = v_1v_2\cdots v_k \Leftrightarrow v_1 = a_1 * u_1, v_{i+1} = v_i * u_{i+1}, \text{ kun } i = 1, 2, \ldots, k-1,$$
$$f_\backslash(v_1v_2\cdots v_k) = u_1u_2\cdots u_k \Leftrightarrow u_1 = a_1\backslash v_1, u_{i+1} = v_i\backslash v_{i+1}. \text{ kun } i = 1, 2, \ldots, k-1$$

Struktuuria $(Q, *, \backslash, a_1, f_*, f_\backslash)$ kutsutaan *kvasiryhmäsalaukseksi joukolle* Q.

Lause 4.2.1. *Olkoon* $(Q, *, \backslash, a_1, f_*, f_\backslash)$ *kvasiryhmäsalaus joukolle* $Q = \{a_1, a_2, \cdots, a_n\}$ *ja olkoon* id_{Q^+} *joukosta* Q *muodostettujen sanojen joukon* Q^+ *identiteettikuvaus. Tällöin*

$$f_\backslash \circ f_* = id_{Q^+}.$$

Todistus. (Vrt. [3, s. 159]). Olkoot $u_i, v_i, w_i \in Q$ ja $k \geq 1$. Olkoot lisäksi $f_*(u_1u_2\cdots u_k) = v_1v_2\cdots v_k$ ja $f_\backslash(v_1v_2\cdots v_k) = w_1w_2\cdots w_k$. Funktioiden f_* ja $f_\backslash$ määritelmistä 4.2.1 saadaan, että $v_1 = a_1 * u_1$, $v_{i+1} = v_i * u_{i+1}$, $w_1 = a_1\backslash v_1$ ja $w_{i+1} = v_i\backslash v_{i+1}$, kun $i = 1, 2, \cdots, k-1$. Nyt lauseen 2.2.2 ominaisuuden 2 nojalla pätee $w_1 = a_1\backslash(a_1 * u_1) = u_1$ ja $w_{i+1} = v_i\backslash(v_i * u_{i+1}) = u_{i+1}$, kun $i = 1, 2, \cdots, k-1$. Täten pätee

$$\begin{aligned}(f_\backslash \circ f_*)(u_1u_2\cdots u_k) &= f_\backslash(f_*(u_1u_2\cdots u_k)) \\ &= f_\backslash(v_1v_2\cdots v_k) \\ &= w_1w_2\cdots w_k \\ &= u_1u_2\cdots u_k.\end{aligned}$$

□

Lauseesta 4.2.1 nähdään, että funktiota f_* voi käyttää salausfunktiona ja funktiota $f_\backslash$ salauksen purkamisen funktiona joukolle Q. Jos siis $u \in Q^+$ on salattava selkoteksti, niin $f_*(u)$ on se salatussa muodossa ja salaus saadaan purettua funktiolla $f_\backslash$, sillä $f_\backslash(f_*(u)) = u$.

Esimerkki 4.2.1. Olkoon joukko $Q = \{a, l, n, s\}$ ja olkoot kvasiryhmän $(Q, *, \backslash)$ laskutoimitukset määritelty siten, että niillä on taulukkojen 4.1 ja 4.2 mukaiset kertotaulut.

*	a	l	n	s
a	a	n	s	l
l	s	l	a	n
n	l	a	n	s
s	n	s	l	a

Taulukko 4.1: kvasiryhmän $(Q, *, \backslash)$ kertolaskun $*$ kertotaulu

\	a	l	n	s
a	a	s	l	n
l	n	l	s	a
n	l	a	n	s
s	s	n	a	l

Taulukko 4.2: kvasiryhmän $(Q, *, \backslash)$ vasemmanpuoleisen jakolaskun \ kertotaulu

Olkoon salattava selkoteksti $u = salasana$. Huomataan, että joukossa Q pätee $a_1 = a$. Salataan teksti laskemalla jokaiselle salattavalle kirjaimelle u_i sitä vastaava salaus v_i. Saadaan

$$f_*(u) = f_*(salasana) = lssnsnnl,$$

sillä

$$\begin{aligned}
v_1 &= a_1 * u_1 = a * s = l,\\
v_2 &= v_1 * u_2 = l * a = s,\\
v_3 &= v_2 * u_3 = s * l = s,\\
v_4 &= v_3 * u_4 = s * a = n,\\
v_5 &= v_4 * u_5 = n * s = s,\\
v_6 &= v_5 * u_6 = s * a = n,\\
v_7 &= v_6 * u_7 = n * n = n,\\
v_8 &= v_7 * u_8 = n * a = l.
\end{aligned}$$

Salatun viestin vastaanottaja tietää, että salauksessa käytettiin kvasiryhmäsalausta $(\{a, l, n, s\}, *, \backslash, a, f_*, f_\backslash)$. Nyt vastaanottaja saa purettua salatun tekstin selkotekstiksi ratkaisemalla kunkin salatun kirjaimen v_i selkokielisen version u_i funktion $f_\backslash$ avulla. Saadaan

$$f_\backslash(lssnsnnl) = salasana,$$

sillä

$$\begin{aligned}
u_1 &= a_1 \backslash v_1 = a \backslash l = s,\\
u_2 &= v_1 \backslash v_2 = l \backslash s = a,\\
u_3 &= v_2 \backslash v_3 = s \backslash s = l,\\
u_4 &= v_3 \backslash v_4 = s \backslash n = a,\\
u_5 &= v_4 \backslash v_5 = n \backslash s = s,\\
u_6 &= v_5 \backslash v_6 = s \backslash n = a,\\
u_7 &= v_6 \backslash v_7 = n \backslash n = n,\\
u_8 &= v_7 \backslash v_8 = n \backslash l = a.
\end{aligned}$$

4.3 Salausalgoritmin arviointia

Arvioidaan seuraavaksi pintapuolisesti, missä määrin edellä kuvattu salausalgoritmi toteuttaa yksityisyyden ja luotettavuuden määritteitä. Koska esitelty salausalgoritmi ei ota kantaa lähettäjän autenttisuuden varmistamiseen, sen arviointi jätetään tässä yhteydessä tekemättä. Tarkastellaan ensin algoritmin luotettavuutta.

Lause 4.3.1. *Olkoon selkoteksti* $u = u_1u_2 \cdots u_k \in Q^+$ *ja olkoon* $v = v_1v_2 \cdots v_k = f_*(u)$ *sen kvasiryhmäsalauksella* $(Q, *, \backslash)$ *salattu muoto. Olkoon lisäksi* $v' = v_1v_2 \cdots v_{i-1}v'_iv_{i+1} \cdots v_k$ *ja* $v'_i \in Q$. *Tällöin*

$$f_\backslash(v') = u_1u_2 \cdots u_{i-1}u'_iu'_{i+1}u_{i+2} \cdots u_k,$$

joillakin $u'_i, u'_{i+1} \in Q$.

Todistus. (Ks. [3, s. 160]). Lause seuraa suoraan salauksen purkamisfunktion $f_\backslash$ määritelmästä 4.2.1. □

Edellä esitetty lause tarkoittaa sitä, että salausalgoritmi on suhteellisen vankka virhetilanteissa. Mikäli siis selkokielen tekstiä salattaessa tapahtuu jokin virhe ja salattuun tekstiin tulee väärin salattu alkio, se ei kaada salausalgoritmia. Tällaisessa tilanteessa on huomioitavaa, että myös salatun tekstin purkamisvaiheessa saatuun uuteen selkotekstiin tulee virheellisiä alkioita, mutta edelleen oikein salatut alkiot ovat säilyneet muuttumattomina.

Tarkastellaan seuraavaksi algoritmin yksityisyyttä. Salattujen viestien yksityisyyttä varjellakseen viestit voidaan pyrkiä lähettää sellaisia reittejä, ettei niitä pystytä lähetyksen aikana kaappaamaan. Algoritmin yksityisyyttä arvioitaessa käsitellään tilannetta, että tunkeutuja onnistuisi kaappaamaan viestin lähetyksen aikana. Algoritmin yksityisyyden kannalta on tärkeää, ettei tällöin tunkeutujan tule pystyä purkamaan salatusta tekstistä selkotekstiä. Pohditaan nyt tilannetta, jossa tunkeutuja onnistuisi kaappaamaan edellä kuvatulla salausalgoritmilla salatun tekstin. Oletetaan että salauksessa on käytetty joukkoa $Q = \{0, \cdots, 255\}$, jota voidaan käyttää esimerkiksi 8-bittisen datan salaukseen. Tällaisia kvasiryhmiä on olemassa huomautuksen 3.1.1 arvion mukaan ainakin $3,05 \cdot 10^{101723}$ kappaletta. Jos tunkeutuja tietää salatun tekstin $v = v_1v_2 \cdots v_k = f * (u_1u_2 \cdots u_k)$, missä $u_1u_2 \cdots u_k$ on tunkeutujalle tuntematon alkuperäinen selkoteksti, niin hänen tulee selvittää salaukseen käytetty kvasiryhmä, jonka avulla salaus voidaan purkaa. Tätä varten tunkeutujan tulisi ratkaista yhtälöryhmä

$$\begin{cases} v_1 = a_1 * u_1 \\ v_2 = v_1 * u_2 \\ v_3 = v_2 * u_3 \\ \vdots \\ v_k = v_{k-1} * u_k. \end{cases}$$

Yhtälöryhmällä on yhtä monta ratkaisua, kuin on kertaluvun 256 kvasiryhmiä. Tästä syystä algoritmi kestää melko hyvin hyökkäyksiä, jotka perustuvat kaikkien mahdollisten salaukseen sopivien kvasiryhmien läpikäymiseen.
Heikkoutena salausalgoritmissa on se, että mikäli tunkeutuja tietää sekä salatun tekstin että selkotekstin, hän pystyy helposti selvittämään salaukseen käytetyn kvasiryhmän $(Q, *, \backslash)$. Tähän varautuakseen selkokielen teksti voidaan salata useaan kertaan ja käyttää toisistaan eroavia kvasiryhmiä.

Tämän aliluvun arviointi mukailee esitetyn kvasiryhmäsalauksen kehittäjien tekemää algoritmin arviointia. [3, s. 159 - 162] Esitelty salausalgoritmi on julkaistu vuonna 1997, minkä jälkeen salausalgoritmille on esitetty vaihtoehtoja ja parannusehdotuksia. Tässä tutkielmassa salausalgoritmin tarkoitus on toimia esimerkkinä kvasiryhmien käytännön sovelluksesta, eikä siten siihen kohdistuneisiin muutosehdotuksiin paneuduta tarkemmin. Aiheesta kiinnostunut voi löytää lisää salausalgoritmin arviointia ja erään muokkausehdotuksen muun muassa lähteestä [6].

Lähteet

[1] J. Dénes and A. D. Keedwell, *Latin Squares and their Applications*, Academic Press, New York, 1974.

[2] C. Kościelny, *Generating quasigroups for cryptographic applications*, Int. J. Appl. Math. Comput. Sci., Vol.12, No. 4, s. 559-569, 2002.

[3] S. Markovski, D. Gligoroski and S. Andova, *Using quasigroups for one-one secure encoding*, in LIRA '97: Proc. VIII Conf. Logic and Computer Science, September 1 -4, 1997, Novi Sad, Yugoslavia, 157-162. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.12.6590&rep=rep1&type=pdf [Viitattu 25.2.2016]

[4] E. Ochodkova and V. Snášel, *Using quasigroups for secure encoding of file system*, Proceedings of the International Scientific NATO PfP/PWP Conference "Security and Protection of information 2001", May 9 -11, 2001, Brno, Czech Republic, 175 - 181. http://spi.unob.cz/papers/2001/2001-24.pdf [Viitattu 25.2.2016]

[5] H. O. Pflugfelder, *Quasigroups and Loops: Introduction*, Heldermann, Berlin, 1990.

[6] V. Scherbacov, *Quasigroup based crypto-algorithms*, arXiv:1201.3016v1, 2012. http://arxiv.org/pdf/1201.3016.pdf [Viitattu 25.2.2016]

[7] J. D. Smith, *Introduction to Abstract Algebra*, Chapman and Hall, United States, 2008.

[8] J. H. van Lint and R. M. Wilson, *A Course in Combinatorics*, Cambridge University Press, United Kingdom, 1992, Second edition 2001.

[9] S. Warner, *Modern Algebra: two volumes bound as one*, Dover Publications, New York, 1990.